

Enhancing reconnaissance security: a 2-tier deception-driven model approach (2TDDSM)

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

¹Department Faculty of Information Technology, College of Engineering, Central Luzon State University, Muñoz, Philippines

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

Article Info

Article history:

Received Feb 16, 2024

Revised Mar 1, 2024

Accepted Mar 10, 2024

Keywords:

Cybersecurity
Deception model
Defense-in-dept
Honeypots
Reconnaissance

ABSTRACT

The emergence of network security has revolutionized the way educational institutions operate, providing advanced connectivity, enhanced communication, and efficient management of resources. However, with the increasing dependence on interconnected systems, institutions and organizations became vulnerable targets for cyber threats. To address these security challenges, a two-tier deception-driven model specifically designed to for the initial phase of attacks in reconnaissance period where the adversaries is to gather information of the targets. Defending threats in this phase can provide active and proactive defense allowing the administrator to identify potential attackers and understanding their methods, motivation and potential target assets. The model's layered approach creates a resilient defense mechanism that aligns with the advanced deception techniques which aims to misguide potential threats attempting to gather intelligence within the network.

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

Muñoz, Nueva Ecija, Philippines

Email: apgamilla@clsu.edu.ph

1. INTRODUCTION

The continuous evolving threat landscape, organization face increasingly sophisticated and persistent cyberattacks that can jeopardize the confidentiality, integrity, and availability of their network infrastructure [1], [2]. As a result, traditional security measures alone are often insufficient to detect and mitigate these threats effectively, hence the continuous evolvement of cyber defense is highly acclaimed [3], [4]. Therefore, the continuous evolution of cyber defense strategies and technologies is highly acclaimed, ensuring that organizations stay ahead of emerging threats and maintain robust security postures. Cyber threats typically differ in their level of sophistication, and not all attacks have the same objective, effect, or impact and a number of general phases can used to break down an attack [5]-[7]. One of ways is applying deception techniques which borrows heavily from military principles by using decoys and lures to mislead attackers into believing they have a foothold in the network and revealing themselves. However, adaptive cyber-defense systems are still in their infancy, and cyber deception is just a small piece of the cyber-defense landscape [8]-[10]. While adaptive cyber-defense systems are currently in their early stages of development, it's important to recognize that cyber deception represents a significant aspect of the broader cyber-defense landscape. One of the part where deception plays a significant role is during reconnaissance phase where threats primary focused is to seek information and potential vulnerabilities, therefore deception techniques introduce the elements of misdirection and misinformation [11]-[13]. Research indicates that prior studies have tended to address only a limited subset of deception tactics, primarily concentrating on the efficacy of

honeypots without adequately attempting to explore additional methods to optimize the reconnaissance phase [14]-[16].

The study explored the impact of two-tier deception security model to improve techniques during the reconnaissance stage, where an attacker tries to gather information about the target network. The layered design offers an additional robust and adaptable solution compared to a single layered design, which primarily focuses on the effectiveness of honeypots; instead, this gives more complexity and makes it more difficult for attackers to bypass the deception. The study covers the effectiveness of applying the two-layered approach in the core layer up to the lower part of the network, which triggers an active and proactive defense by actively engaging with attackers during the reconnaissance phase.

2. METHOD

The study was structured into two main phases: an initial setup involving the addition of scripts and policies to lure and gather intelligence on potential intruders, followed by an evaluation phase to assess the efficacy of these measures. The evaluation includes a comparative analysis between traditional and deception-based network configurations through the use of network tools to ensure the reliability of test outcomes. This enabled a comprehensive examination of the effectiveness of deception techniques in enhancing network security.

2.1. Two tier deception security experimental setup

The test bed network was composed of building a network that was used when handling a large number of users. The Figure 1 shows that the setup was built starting with the core router configuration and then adding a core switch to handle the division of the network at the lower level of the network. The layer 2 consisted of a deception controller, where traps and decoys would serve as the active approach to luring the threats. The setup focused on the core layer of the network, which plays a major role in controlling threat penetration by directly implicating the requirements required before the packets reach deep into the network. The core device was used to implement a deception approach and test packet flows to lure the attackers. The applied scripts and rules were added to manipulate the flow of the packets, deceiving the perpetrators and recording the events happening inside the network. The approach is designed to systematically evaluate the effectiveness of deception techniques within the core network. A strategic deployment of policy to observed attacker's behavior aim to assess the practical implications and feasibility of integrating deception tactics into network configuration strategies based on how network address translation (NAT) policy works. The second layer directly controls the flow in the internal network, which applies the techniques of deception security. In order to test the effectiveness of the implemented techniques, a test node was deployed in the core router and in the layer 2, where decoys and traps were strategically distributed.

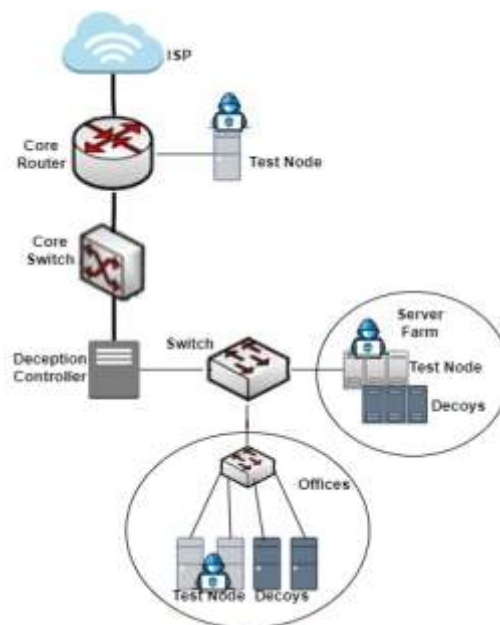


Figure 1. Test bed network diagram

2.2. Network test evaluation

To test the effectiveness of two controlled testing environments, one utilizing a traditional network design without deception techniques and the other incorporating a two-layered deception architecture, this is evaluated based on the NMAP test results, which is a powerful network scanning tool that provides valuable information about network hosts, open ports, services, and operating systems. NMAP scans networks for active hosts and provides services using the known sequence of the OS's TCP/IP handshakes. In order to distinguish between the networks of wired and wireless services, NMAP employs a technique called OS fingerprinting. The tools were deployed in different parts of the network, such as the core layer and the lower part of the network. With these, this gives several ways in examining the network with the tool to get a more accurate way to study the effectiveness of the deception techniques.

3. RESULTS AND DISCUSSION

The controlled experiments involved deploying the two-tiered model within the test bed network to evaluate its threat detection capabilities and assess attacker engagement. The experiments measured the effectiveness of deception techniques and compared the resilience of the two network environments, providing insights into their security posture. This shows the effectiveness of the deception security model, highlighting the security in the reconnaissance phase.

3.1. Component's background

This section explores how the two-tier deception layered network flow and deceptive countermeasure enhances network security. It also discusses firewall NAT rules, which manage network traffic and enforce security policies. Together, these components form the foundational elements of the network's security infrastructure.

3.1.1. Two tier deception layered network flow

The Figure 2 shows the algorithm how the layer 1 defense controlled the traffic flow of the intended attacks when penetration testing occurs. Layer 1 acts as the road-map for the packets to make sure that all legitimate payloads will access the server. When the core router received payloads, the chain criterion must be satisfied which served as filtering techniques where we know that the payloads was randomly send only by the attackers from the gathered intel in the reconnaissance phase. If the attackers were successfully satisfied the criterion, another criterion needs to meet before it proceeds to the layer 2 of filter in the lower level of the network. To fully utilize the core router defense, predetermined bait addresses were added to create an initial log of the perpetrator's malicious intent. Layer 2 controls the deception flow of the packets. Creating traps to lure the attacker, such as setting up multiple decoys (DB server, SNMP, telnet, web-server, ssh) [17], [18]. This gives a clear view of the purpose and methods of the perpetrator and traces the root cause of the attack.

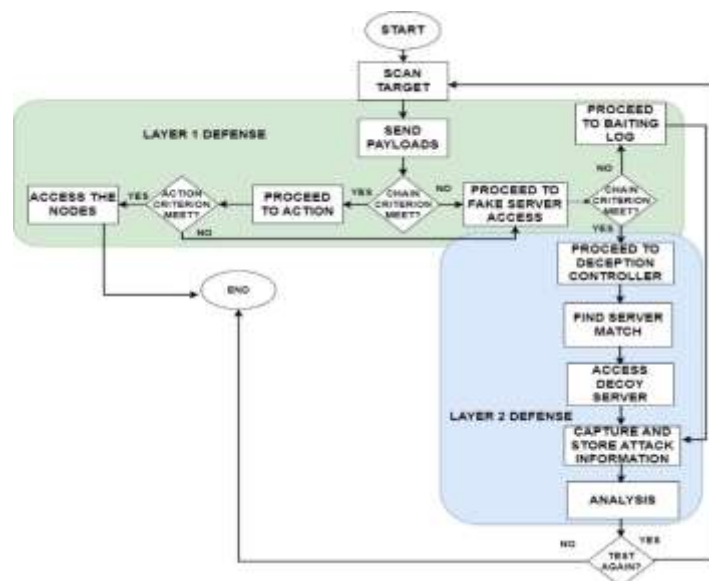


Figure 2. Deception-driven security model packet flow

3.1.2. Firewall NAT rules

The NAT rules above shows the restriction that was imposed to the router mainly controlling the flow of the packets. The core layer plays a vital role in executing the proposed model particularly the router that communicates between the internet and the devices in the network. Figure 1 illustrates the method used to prevent the intruder from penetrating deeper into the network and instead directing them to the lure setup using deceptive routing techniques. The scripts focus on creating firewall rules for network address translation (NAT), mapping legitimate assets to decoys and traps [19]. The script includes two parts: CHAIN and ACTION. The chain permits a packet to be matched against a common criterion in one chain (one rule) and then passed to another chain for processing against a different set of common criteria. For instance, a packet should be compared to the IP address: port. When the packets are matched by the rule, it will forward to the ACTION and perform the created rules for the packets. When mapping the chain for legitimate nodes, set connection-Nat-state to dstnat to allow the packets to transmit to a specific server, then assign your router's WAN address, and align with the specific protocols and ports. Include dstnat as the action and add the address and port of your servers. This restricts server traffic to only legitimate requests. To lure the attackers, the script above directly controls the flow of traffic to more open and visible traps. To effectively deceive attackers before they reach the server, directly mapping decoys to the router expedites the deceptive flow during reconnaissance. Similar to legitimate applied rules, we must establish a dstnat and its address, but instead of allowing it to flow freely within the internal network, the packets will go directly to the bait address, where the defender can examine and evaluate the attacks. In addition, if you do not wish to configure a decoy server, you can construct the bait directly on the router by applying the bait's address and generating logs that detail the attack. Please note that the effect of the chain rules is taken in the order they are listed from top to bottom, legitimate scripts must be at the top in order to prioritize legit packets to travel in the network without any problems. Since the chain and action must meet the requirements of the action, this gives them a hard time to scan and get the proper combination of address and port; hence, all the attacks go to the decoy server.

Legitimate Server: Chain{

```

dstnat
  WAN address: 192.168.x.x
Port: 80
Action {
  dstnat
    Server IP address: 192.168.x.x
    Access Ports: 80
  } }

```

Fake Server: Chain{

```

dstnat
  WAN address: 192.168.x.x
Action {
  Deception Controller IP address: 192.168.x.x
} }

```

Setup bait logs: Chain{

```

dstnat
  bait Address: 192.168.x.x
Action {
  log
}

```

Implementing multiple security measures in different levels ensures that if one layer of security is breached, there is still another layer of protection to prevent unauthorized access or mitigate the potential damage. This leads the primary focus of the layered 2 to improve the defense in-dept model, the active security deception or active defense is a proactive security strategy that involves intentionally misleading and confusing potential attackers to detect, divert, and deter them from their malicious activities. A deception-based security where organizations actively create decoys, traps, and false information to deceive attackers. Active security deception goes beyond passive defense mechanisms, such as firewalls and intrusion detection systems, by actively engaging with attackers and luring them into controlled environments. The model focused on the deceptive network architecture where we intentionally mislead attackers and using decoy systems and fake services. Attackers was led to believe they have successfully compromised legitimate systems when, in reality, they are operating in an isolated and controlled environment.

Since most of the time it redirects and created a bait address that doesn't need to meet the three-way handshake process. It prevents the use of two much resources of the devices. Understanding what to put in the parameters such as the protocol, ports and addresses plays a big role on how to deceive and lure the attackers.

3.1.3. Deceptive countermeasure results

The deceptive DNC in Table 1 are security techniques that use the misleading traits that were mapped from the framework for deception to strengthen the network map [20]-[22]. The researcher used this to split of work into two layers was implemented in the network by dividing it into passive security, which is primarily designed to prevent unauthorized access requiring continuous active intervention, and active security, which proactively detects, responds to, and mitigates security threats in real-time. These countermeasures serve as a mask, mimicry, decoy, camouflage to add confusion and used the reconnaissance period as a reverse technique as it was used as an advantage by the defender to exploit the attacker and understand its goals and purpose. This matrix countermeasure reflects how the division of the countermeasure into different layers can be effectively distributed in order to not put much process load on the devices in the network infrastructure. This can avoid too much overload and conserve device resources without putting too much burden on the network.

Table 1. Network matrix of deceptive countermeasure

Network countermeasure	Passive		Active	
	Static	Dynamic	Static	Dynamic
Faked OS			√	
Fake Network Topology		√		
Faked TCP/IP Stack	√			√
TCP/IP Fingerspoofing			√	
Faked Services			√	
IDS logging	√		√	
IDS alerting		√		√
Fake Database			√	

3.2. Test results

The test results stemmed from an attempt to initiate an attack within the network as shown in the test bed network diagram, commencing from the reconnaissance phase where the attackers sought to gather information on open ports, IP addresses, and other vulnerabilities within the network. Upon receiving the attack payload. The results demonstrated the effectiveness of the two-tiered deception techniques in luring the attackers.

3.2.1. Deceiving perpetrators

Deception techniques were highly commended to boost security for systems and components through denial, deceit, misinformation, camouflage, and obfuscation [23]. As Sun Tzu once wrote, "all warfare is based on deception", which emphasizes that deception is a fundamental element in achieving victory and gaining strategic advantages over opponents [24], [25]. The Figure 3 shows that as the reconnaissance was commencing the network created a pool of legitimate and illegitimate pool of IP addresses from different parts of the network started in the connected nodes in the core upto the lower level of the network in the server farm and offices resulting of misleading the enemy, concealing intentions and plans, feigning weakness or strength, diverting attention and resources, and trying to get them back by exposing their weaknesses by intentionally providing false information or creating a false narrative, defenders can manipulate the enemy's perception. This shows that the applied setup that was discussed above effectively created and lure the attackers giving more time for the administrator to assess and enhance mitigation of the intended attackers.

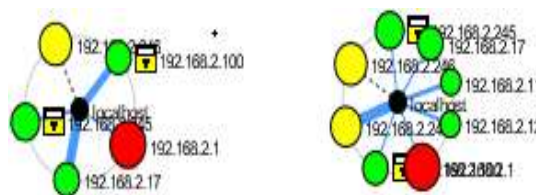


Figure 3. Traditional vs deception-driven security-based model

3.2.2. NMAP test results

The experiment conducted in a traditional and deception applied network that targets the port and addresses in the network. This was evaluated by six (6) types of scans: TCP connect that sends SYN/ACK packet, half scan for RST packets, UDP to test a stateless nature, Null for the packets that has no flags set, FIN for fin flag and Xmas to test TCP packets with the PSH, URG and FIN flags set. Different scan types represent a comprehensive evaluation of network resilience against different type of payload and packet distribution.

The Figure 4 depicts a comparison of the traditional and the improved network design in shielding the important assets through deception. The test was conducted into six types of NMAP scans that checks difference paths of sending packets and receiving packets and the dept. of exploring the network. This is worth to remember that the primary goal of deception techniques in a security model is to enhance the security posture of a network by misleading and confusing potential attackers [26], [27]. Each type of scans was used different techniques of sending packets with different flag set towards the ports and addresses and the applied model almost provides 40 to 50 percent traps that can give more headaches to the attacker and gave more opportunity for the defender to examine the intruders goal. The test shows that the attackers were surrounded by more deceptive scheme which gives them a more confusing and time-consuming attacks applying deception model compared to the traditional method. Thus, the results of different tests where it handled different ways of packet distribution and target ports and addresses show a consistent output that the new design model gives a more deceptive chance for the attacker. By combining the first layers of lured action, it decreases the chance of almost 80 percent in finding the true assets.

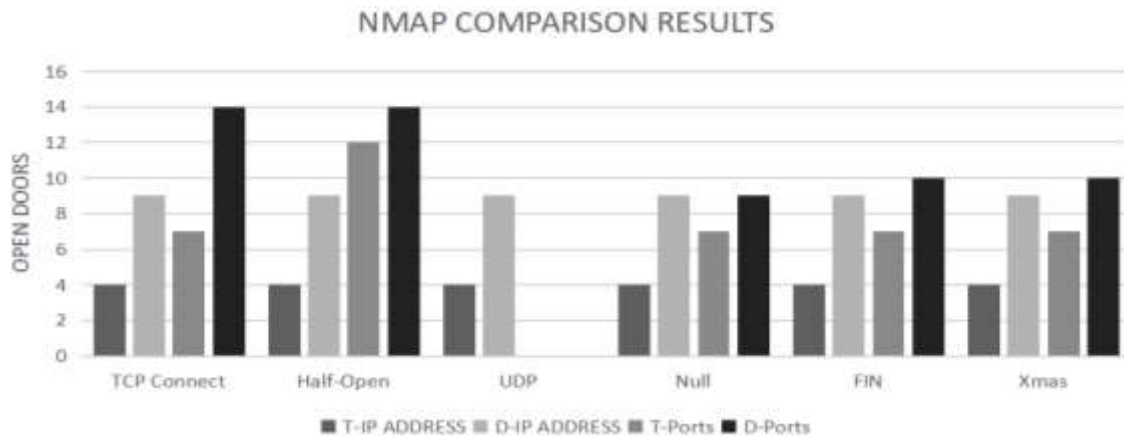


Figure 4. NMAP scans comparison

The result of the tests above demonstrated that the proposed deception model shows an effective result in handling attackers from the first layer where the core layer act as a deceiving path for the attackers not sacrificing resources. As the attackers goes the next layer of defense also created a barrier of fake doors to deceived them and give them false information as they gathered information in the reconnaissance period. This offers a thorough and tiered security strategy by combining passive deception in the first layer and active deception in the second layer. Therefore, it can be observed that the suggested approach is highly successful in drawing them in and tricking them into going to traps and fake doors, which initially supports the administrator by enabling them to see the attacker's footprint. These methods serve as early warning systems, allowing the detection of suspicious activity and giving important information about the tactics and goals of the attackers. Organizations can distract and delay attackers, making it harder for them to accomplish their objectives, by providing fake targets, misleading network topologies, and misleading information.

Based on the findings presented, future research could explore several approaches, and one potential direction involves investigating the integration of machine learning algorithms to dynamically adapt deception strategies. The research could focus on refining the deception techniques employed in each layer of defense and increasing attacker engagement with decoy assets. Overall, these future studies aim to further enhance the effectiveness and practicality of deception-driven security strategies for organizations facing increasingly sophisticated cyber threats.

4. CONCLUSION

The two-tiered deception security model provides a well-built defense against malicious threats that gives administrators a plan to strengthen network safety by seamlessly integrating active and passive deception tactics across multiple layers. The results demonstrated that the configured scripts and policies successfully lured and deceived the attackers by filtering the payloads at every network layer as a part of reconnaissance phase. This strategy not only discourages attackers but also gives administrators insightful information to improve their mitigation and security posture. Organizations can efficiently deter attackers and strengthen their defenses against threats by utilizing fake targets, deceptive network topologies, and misdirection. The findings provide conclusive evidence that, by taking a proactive approach, administrators can prevent security lapses and protect vital components of the network architecture.

ACKNOWLEDGEMENTS

The authors would like to thank the Central Luzon State University Information Systems Institute for allowing us to use their infrastructure and network equipment for the development and testing of our experiments.




REFERENCES

- [1] P. Institute, "The human factor in data protection," 2012. [Online]. Available: http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf.
- [2] P. Institute, "Threat intelligence & incident response: a study of U.S. & EMEA organizations," 2014. [Online]. Available: https://www.ponemon.org/local/upload/file/AccessData_Report_Final.pdf.
- [3] X. Han, N. Kheir, and D. Balzarotti, "Deception techniques in computer security," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, Jul. 2019, doi: 10.1145/3214305.
- [4] D. Liebowitz *et al.*, "Deception for cyber defence: challenges and opportunities," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, IEEE, pp. 173–182, Dec. 2021, doi: 10.1109/TPSISA52974.2021.00020.
- [5] W. Mazurczyk and L. Cavaglione, "Cyber reconnaissance techniques," *Communications of the ACM*, vol. 64, no. 3, pp. 86–95, Mar. 2021, doi: 10.1145/3418293.
- [6] J. Haseeb, "Deception-based security framework for IoT: an empirical study," Open Access Te Herenga Waka-Victoria University of Wellington, 2023. doi: 10.26686/wgtn.21965195.
- [7] S. Sugrim *et al.*, "Measuring the effectiveness of network deception," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, Nov. 2018, pp. 142–147. doi: 10.1109/ISI.2018.8587326.
- [8] A. Bushby, "How deception can change cyber security defences," *Computer Fraud & Security*, vol. 2019, no. 1, pp. 12–14, Jan. 2019, doi: 10.1016/S1361-3723(19)30008-9.
- [9] K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major, "Game theory for adaptive defensive cyber deception," in *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, New York, NY, USA: ACM, pp. 1–8, Apr. 2019, doi: 10.1145/3314058.3314063.
- [10] A. Farar, H. Bahsi, and B. Blumbergs, "A case study about the use and evaluation of cyber deceptive methods against highly targeted attacks," in *2017 International Conference On Cyber Incident Response, Coordination, Containment & Control (Cyber Incident)*, IEEE, pp. 1–7, Jun. 2017, doi: 10.1109/CYBERINCIDENT.2017.8054640.
- [11] I. Belalis, G. Spathoulas, and I. Anagnostopoulos, "Modeling intruder reconnaissance behavior through state diagrams to support defensive deception," *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, pp. 275–302, Jun. 2023, doi: 10.3390/jcp3020015.
- [12] W. Tounsi, "Cyber deception, the ultimate piece of a defensive strategy - proof of concept," in *2022 6th Cyber Security in Networking Conference (CSNet)*, IEEE, pp. 1–5, Oct. 2022, doi: 10.1109/CSNet56116.2022.9955605.
- [13] J. Pawlick and Q. Zhu, "A taxonomy of defensive deception," in *Game Theory for Cyber Deception*, pp. 37–48, 2021, doi: 10.1007/978-3-030-66065-9_4.
- [14] A. S. Demochkin and A. P. Ivanov, "A survey of software implementation for high-interaction honeypot technologies," *Engineering and Technology*, no. 1, 2021, doi: 10.21685/2587-7704-2021-6-1-9.
- [15] Z. Lu, C. Wang, and M. Wei, "A proactive and deceptive perspective for role detection and concealment in wireless networks," in *Cyber Deception: Building the Scientific Foundation*, Cham: Springer International Publishing, pp. 97–114, 2016, doi: 10.1007/978-3-319-32699-3_5.
- [16] S. Hassan and R. Guha, "Modelling of the state of systems with defensive deception," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, pp. 1031–1036, Dec. 2016, doi: 10.1109/CSCI.2016.0197.
- [17] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021, doi: 10.1109/COMST.2021.3106669.
- [18] N. Alhosani, S. Alrabae, and A. Al Faresi, "An efficient strategy for deploying deception technology," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, pp. 177–194, 2024, doi: https://doi.org/10.1007/978-3-031-50051-0_13.
- [19] D. Kusumadihardja, "Fools your enemy with MikroTik." Slideshare a Scribd company. Accessed: Feb. 15, 2024. [Online]. Available: <https://www.slideshare.net/zonicorb/fools-your-enemy-with-mikrotik-67235380>
- [20] S. Yek, "A deception based framework for the application of deceptive countermeasures in 802.11b wireless networks," Palgrave Macmillan UK, London, 2023, doi: 10.1057/978-1-349-96073-6_427.
- [21] M. A. Naagas, E. L. Mique Jr, T. D. Palaoag, and J. S. Dela Cruz, "Defense-through-deception network security model: securing university campus network from DOS/DDOS attack," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593–600, Dec. 2018, doi: 10.11591/eei.v7i4.1349.
- [22] V. E. Urias, W. M. S. Stout, and H. W. Lin, "Gathering threat intelligence through computer network deception," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, IEEE, pp. 1–6, May 2016, doi: 10.1109/THS.2016.7568916.




- [23] 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, Dec. 2021, doi: 10.1145/3450973.
- [24] L. Giles, "Sun Tzu the art of war the oldest military treatise in the world," Allandale Online Publishing. [Online]. Available: https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf.
- [25] A. Networks, "Deception technology: a critical component of a modern cyber security stack," SentinelOne. [Online]. Available: <https://www.sentinelone.com/resources/deception-technology-a-critical-component-of-a-modern-cybersecurity-stack/>.
- [26] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-rehman, "Penetration testing active reconnaissance phase - optimized port scanning with nmap tool," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, Jan. 2019, pp. 1–6. doi: 10.1109/ICOMET.2019.8673520.
- [27] K. T. Andrews, "Deception techniques and technologies in the role of active cyber defense," 2020. [Online]. Available: <http://search.proquest.com/pqdtlocal1008803/docview/2469314657/abstract/F1B43D01AB6B48B6PQ/13>

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.



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.



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 ICCT, ACM ICCBN, ACM ICNCT, IJEECS, and IRCITE. He can be contacted at email: manaagas@clsu.edu.ph.