Dynamic Network Simulation Methodology

CS4991 Capstone Report, 2022
Daniel Lower-Basch
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
dgl5vnh@virginia.edu

Abstract

Noblis wanted to expand its simulation capabilities for network research. I developed simulations of a dynamic network as a baseline against which to compare defense methods to determine metrics of success. I researched the network simulation software available to me and acceptable to a government contractor like Noblis. The result was the decision that Cisco Packet Tracer was the best fit for the combination of requirements and available skill level. The end result was a simulated network with inbuilt packet traffic. Future work should include the integration of the defense methods being tested into the simulated network.

1. Introduction

The consequences of cyber warfare can include government systems being overthrown, extensive human casualties, severe damage to the national economy, and the initiation of physical warfare (1). As we integrate technology into more aspects of our lives, the dangers of lacking network security become greater. Noblis is working on developing defense methods based on the idea of moving target defense (MTD). Depending on how a network is configured, there are different ways that hackers can attack. The attack surface of a network is made up of the system resources exposed to attackers, including communication ports, publicly sourced software, or component vulnerabilities (2). The idea behind MTD is that these attack surfaces can be regularly changed by cycling the network through dynamically generated configurations of differing structure but equal efficiency (4). Research has been done on the adaptive use of network defense mechanics, but MTD was not included (3). As such my internship was created to determine how difficult it would be to implement Adaptive MTD.

The benefit of MTD is that it reduces the inherent advantages attackers hold. Attackers will always have the ability to study networks they mean to attack and to choose the time of attack for their maximum benefit (2). MTD regularly changes the network, meaning that studying the network will only help until the next shift. This means that attacks take more time and are more likely to trigger defense mechanisms, which means that the overall attack is less likely to succeed. However, nonadaptive MTD has the disadvantage that it does not take the attacker into account when it shifts. Adaptive MTD seeks to overcome this weakness by including the feedback from other defense mechanisms into its inputs. While this has the potential to greatly increase the security potential of MTD, we do not know the

tradeoffs in terms of the ease of use of networks where Adaptive MTD is implemented. Thus, my internship involved working on simulating the effects of Adaptive MTD on a network in terms of security and ease of use.

2. Related Work

1. Li and Liu (2021) defines the terms cyber-attacks and cyber security in greater detail, along with the effects of both. This was important to my project because it helped me to define the need for further developments in network security.
2. Zhuang, et. al. (2012) provided one of the primary inspirations for my project. They researched simulating the effects of a nonadaptive MTD on network security and ease of use. My project is meant to expand upon their work to include adaptive MTD.
3. Atighetchi, et. al. (2003) provides the rationales behind defense on the network level, and a number of methods for how attackers and defenders act on a network level. It was very helpful in developing my understanding of how an implemented adaptive MTD would function, and how to simulate such a defense mechanism.
4. Cho, et. al. (2020) discusses the different ways MTD are implemented depending on their environment, requirements, and methodology. It was very useful in defining what does change between nonadaptive MTD and adaptive MTD, and what does not.

3. Project Design

To start, I was provided with a number of different articles on MTD and asked to come up with a project design similar to the one covered in Zhuang, et. al. (2012) for usage with adaptive MTD.

3.1. Initial Design

The goal of my project was to test the effects of adaptive MTD on defense and quality of service. To achieve this goal, my initial plan was to follow the example of Zhuang, et. al. (2012) in creating a simulated network using NeSSi2. The idea was to have a section of the network defined as the user network, a section that would perform a simulated attack, and a section that would act as a network controller to simulate adaptive MTD, as well as a way to record the results. The metrics of success were the time it took for packets to reach their destination for quality of service, and the percentage of attacks prevented and how long the successful attacks took for the quality of defense. To achieve this I needed a network, a way to generate network traffic, and a network controller.

3.2. Security Requirements

Noblis is a government contractor, meaning that they have sensitive information on their network. As such, security was important for everyone, even those who were not working directly on the sensitive information. Anyone connected to the network could potentially cause a security leak, which meant that I could not directly download NeSSi2, an open-source software, onto my company laptop. To satisfy the security requirements, I requested that an edge virtual machine (VM) be provisioned in Noblis' cloud environment. By doing so I created a limited environment for the open-source software, meaning that any attempts to infect the network could easily be detected and shut down by deleting the VM with minimal backlash on the rest of the network. X11 forwarding allowed for the connection of my laptop and the edge VM, and if I did not have enough computing ability, I could always requisition more due to it being a VM in a cloud environment.

3.3. Complications

The first major complication came about as a result of the fact that NeSSi2 is an outdated network simulator. It has not been updated since 2013, meaning that when a problem arose due to the interaction between the edge VM, the Java environment, and NeSSi2, there was no recent documentation to get the

help needed to fix the issue. After some time trying to resolve the issue, I made the decision to look into alternative network simulation software that was more recent. As a result, I found GNS3 and Cisco Packet Tracer. My next attempt was with GNS3, as it is more customizable than Cisco Packet Tracer. As GNS3 is another open-source software that Noblis does not trust, I reused my edge VM environment, and successfully developed a simulated network. The next complication was in generating network traffic. GNS3 does not have the inherent function to generate network traffic, and the external application that could do so required a paid subscription, and was not approved by Noblis. As such, I switched to my final platform, Cisco Packet Tracer.

3.4. Final Design

Cisco Packet Tracer is a Noblis trusted software, meaning that I could use it directly on my company laptop instead of the edge VM, speeding up progress substantially. Additionally, Cisco Packet Tracer has the inbuilt ability to generate scheduled network traffic on a simulated network. As such, I created a network with four routers, all interconnected, and three of those routers connected to two users each. Each of those users is scheduled to ping each other user in sequence.

4. Results

The results of the designed scenario were that the pings with a shorter network distance finished sooner, but all pings finished relatively quickly. Noblis will presumably use the created scenario as a base to compare more complicated scenarios against in determining whether adaptive MTD is a worthwhile investment. The anticipated outcome of introducing malicious packets into the current network is that the defensibility is very low, but that the quality of service is high, and introducing adaptive and nonadaptive MTD to the network will increase the defensibility at the cost of the quality of service. To what degree I do not know, as that is what the project was designed to find out.

5. Conclusion

This project developed a base network for Noblis to reference against as a control when developing more complex networks. This will allow for those who follow up to have a foundation to work with when developing more dynamic network simulations. While we did not finish the path we set out to walk, we made a trail for those following in our footsteps.

6. Future Work

The next step with this project would be to implement methods for simulating the usage of both adaptive and regular MTD while recording the effects on both security and quality of use. By doing so we will show the potential adaptive MTD has in comparison to current security methods.

7. UVA Evaluation

UVA prepared me for this internship well, with Network Security teaching me the seven layers of networks and how packets and security interact with these layers. However, I was not well prepared for actively simulating networks, as shown by my difficulties in identifying network simulation software that matched my needs. I have not yet taken the Computer Networks course, so my opinion may change after doing so. As of right now, I would recommend the addition of network simulation to the curriculum. We are given a strong theoretical base of knowledge on how networks work, but less practical knowledge, which the inclusion of network simulation could help with.

8. Acknowledgements

I would like to recognize my manager, Janine Tucker, who was the developer of the idea behind this research internship. She got me in contact with both academic articles and fellow employees to help resolve my questions and difficulties. Without her, this project would never have been possible.

References

1. Yuchong, L., & Qinghui, L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 7. 10.1016/j.egyr.2021.08.126.
2. Zhuang, R., Zhang, S., DeLoach, S., Ou, X. and Singhal, A. (2012), Simulation-based Approaches to Studying Effectiveness of Moving-Target Network Defense, National Symposium on Moving Target Research, Annapolis, MD, US, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=911408 (Accessed September 19, 2022)
3. Atighetchi, M., Pal, P., Webber, F. and Jones, C. "Adaptive use of network-centric mechanisms in cyber-defense," *Second IEEE International Symposium on Network Computing and Applications, 2003. NCA 2003.*, 2003, pp. 179-188, doi: 10.1109/NCA.2003.1201154.
4. Cho, J., Sharma, D.P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T.J., Kim, D.S., Lim, H., & Nelson, F.F. (2020). Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. *IEEE Communications Surveys & Tutorials*, *22*, 709-745.