Impact of a DDoS Attack on Computer Systems: An Approach Based on an Attack Tree Model

Ronierison Maciel*, Jean Araujo†‡, Jamilson Dantas*, Carlos Melo*, Erico Guedes*, and Paulo Maciel*
*Informatics Center, Federal University of Pernambuco, Recife, Brazil
†Academic Unit of Garanhuns, Federal Rural University of Pernambuco, Garanhuns, Brazil
‡NOVA LINCS & DI, FCT, Universidade NOVA de Lisboa, Caparica, Portugal
{rsm4, jrd, casm3, eacg, prmm}@cin.ufpe.br, jean.teixeira@ufrpe.br

***Abstract*—Attacks that deny access to a service provider can occur anytime, anywhere, and most usually occur with little or no warning. Many small and midsize companies are not prepared to handle a significant outage. For an enterprise to face up to an attack of this type, it must possess a bandwidth higher than that of the attack, an infrastructure with redundant components, regular backups, firewalls for monitoring the threats and other proactive and reactive mechanisms. Otherwise, the service will be interrupted, increasing the chances of financial losses. Hierarchical modeling approaches are often used to evaluate the availability of such systems, thereby leveraging the representation of multiple failure and repair events in distinct parts of the system. This paper evaluates the impact of a distributed denial-of-service attack in computer systems. We propose hierarchical models that represent the behavior of major system components and assess the effects of a DDoS attack on the system availability. The equations that estimate the likelihood of an attack, attacker benefits, feasibility, the pain factor and the propensity of the offense were present. They enable a direct analytical solution for large systems. The results obtained from the attack tree analysis allow to plan and improve system's availability, maintainability, and reliability. The attack tree indices show the impact of simultaneous attacks on a computer system and the several threats which will maximize the system downtime.**

Keywords*—*Attack Tree, Security, Threats, Modeling, Distributed Denial-of-Service

I. Introduction

Computing infrastructure depends on various fault tolerance mechanisms to cope with software and hardware failures so that, as users expect, resources are accessible anywhere and anytime [1]. However, several factors can cause a system to be unavailable. One example is the Distributed Denial-of-Service (DDoS) bots [2]. At the end of 2016, Dyn's DNS [3] faced catastrophic events. Many systems like Twitter, Spotify, and SoundCloud were inaccessible for two hours.

The DDoS method came to notice in 1997 [4]. It misrepresented legitimate access, resulting in several problems to victims, such as customer losses, financial issues, losses of credibility and other factors that result in a system undergoing downtime [5]. Virtual threats are increasing, becoming more sophisticated and representing a growth destruction power. It is was estimated that only 7% of companies in the world could monitor, detect and prevent virtual threats. The was extremely alarming, as the remaining 93% of companies are subject to catastrophic corruption by virtual threats [6]. Malicious activities result in losses for enterprises, data centers management, health systems, and real-time operating systems. An example of a global ransomware attack is WannaCry [7]. So systems must be analyzed to mitigate the impacts of possible failures on its dependability.

Studies have been conducted to verify the effectiveness of Attack Tree (AT) analysis in computational infrastructures. Using attack tree, Roy [8] proposed attack cost and attack likelihood techniques to evaluate a SCADA system. Mauw and Oostdijk [9] showed the specific foundations of an attack tree and its particularities. Schneier [10] brings aspects that characterize attack trees, such as attack cost and the probability of occurrence. Edge et al. [11] proposed a framework for modeling, analysis, and mitigation of threats using attack tree. However, from attacks, no study presents how to analyze several threats using DDoS. Furthermore, most papers available in the literature do not have a broad coverage of threats.

This paper presents strategies to evaluate the likelihood of attack, the financial losses of victims, the attacker's benefits, the feasibility of an attack, the pain factor and the propensity of an attack using DDoS techniques. The goal is to assess availability, as represented by Attack Tree. The evaluated system follows a baseline architecture with a robot network (botnets) of attack. This evaluation shows the threats that would have the most significant impact on the downtime of a system.

The remainder of the paper is organized as follows. Section II presents an overview of DDoS methods and the conceptual knowledge regarding Attack Tree. Section III presents the attack tree model used and describes the definition of user and attacker profiles. Section IV presents the results obtained from the model. Finally, Section V makes some closing remarks, discusses the primary results and indicates future lines of research.

II. Background

This section describes the most common DDoS attacks and the central concepts of attack tree modeling.

A. Distributed Denial-of-Service (DDoS)

Figure 1 shows behavior the DDoS attack. The attacker holds control of servers (zombies) connected a computer's network. The primary objective of the attacker is to saturate the bandwidth of the victim.

One of the programs most used for this type of attack is called Backdoors [12]. Backdoors is a malicious software

978-1-5386-3664-0/18/$31.00 ©2018 IEEE

that infects the victim and provides full access to the user's computer and its resources, which means it can get the computer to perform tasks in its favor. Given these circumstances, the computer becomes part of a robot network (botnets), an abbreviation for computers that perform illicit activities which the user does not know of, commonly known as, a zombie computer network [13].

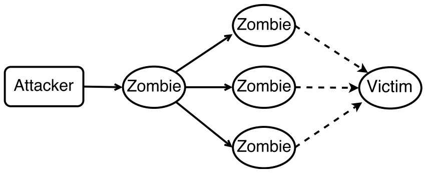


Fig. 1. Example of a DDoS attack

Commonly known as Layer 7 attacks, application attacks are designed to overload specific services during its execution. This type of attack can be carried out on a single machine and resembles legitimate user traffic, which hampers being able to mitigate it. Its primary objective is to destabilize or freeze the victim's computer or service by sending malformed or large packets, overloading the target device [14].

The main feature of the protocol', exploit attack' is to probe implementation errors of some protocols running on the victim's machine, to overburden its processor and hard-disk resources [15] completely. In flood attack, a high volume of traffic is sent to a system which does not perform any examination of the received packets [16]. The purpose of reflection-based volumetric attacks is to exhaust the capacity of the available bandwidth of a specific company. The attackers have botnets to generate a large volume of traffic in victim network: machines are illegally taken over by backdoors viruses to amplify this type of attack [17].

B. Attack tree modeling

Security specialists have been discussing how to prevent interruptions to business continuity due to the occurrence of virtual attacks. The attention to these discussions has been drawn not only in the specialist literature but also widely in the general media. Given the potential scale of financial losses, organizations must adopt strategies to mitigate these threats. Moreover, there have been advances in technology and mechanisms to create protections against these threats.

Attack Trees(AT) [10] is an emerging and promising approach that aims to reduce financial losses by mitigating threats [18]. AT solutions are beneficial as they can produce notifications regarding computational threats in organizations. The ways to do this include: (1) assigning probabilities of occurrence to significant known risks; (2) analysts can model the attacker's behavior and can calculate how long it takes for the attacker to subvert a system; (3) The analyst should also advise how much the victim should invest to avoid some type of attack on its infrastructure. With this information, it is possible to evaluate the security built into a model with higher refinement as to potential threats.

The representation of an AT is structured and hierarchically distributed, as shown in Figure 2. Attack Trees adopt a bottom-up approach. We start from the leaf nodes, in which malicious activities are performed. Then, the logical operators OR or AND are used to model the joint effects of the considered attacks. A further computation is made for each logical operator to reach the attacker's primary objective finally.

The probability of a successful attack of an AND gate, modeled in an attack tree, is calculated by Equation (1). The probability of a successful attack of an OR gate is calculated by Equation (2). Both equations are defined in the interval $[0, 1]$. n represents the number of child nodes in the tree, and Likelihood of Occurrence (LoO_i) represents the probability of a successful attack [19].

$$P_{AND} = \prod_{i=1}^{n} LoO_i \tag{1}$$

$$P_{OR} = 1 - \prod_{i=1}^{n} (1 - LoO_i) \tag{2}$$

There are tools [20], [21] that can automate the whole process of threat investigating through the adoption of ATs. In complex models, there will be several additional leaf nodes and logical operators. In these cases, the adoption of these tools will accelerate the performed investigation.

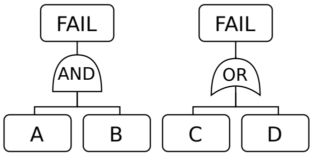


Fig. 2. Example Attack Tree

III. Proposed approach to DDoS attack analysis

This section presents the adopted proposal to analyze the main DDoS attacks methods using attack tree.

One of the first tasks in an experimental study is to state the aimed goals and how we may reach them. So, it is need to define a list of main breach threats to evaluate the behavior of any computing system whose security was broken. The considered risks should be relevant to the experiment. After listing the main threats, we must state a way to obtain the needed information. To achieve that, we model an attack tree using SecurlTree tool. It provides a flexible method to generate results regarding the system security behavior. Figure 3 shows a chart that summarizes the adopted strategy. The presented activities are described below.

Understanding the actual infrastructure: a broad assessment of the primary attack techniques for trace the attacker and victim profiles is performed. It encompasses the attackers and victims behaviors.

Modeling Attack Tree: it defines the model and logic structure of the system, as well as the DDoS attack techniques. After AT model development, there is a subprocess formed by two activities, as described below.

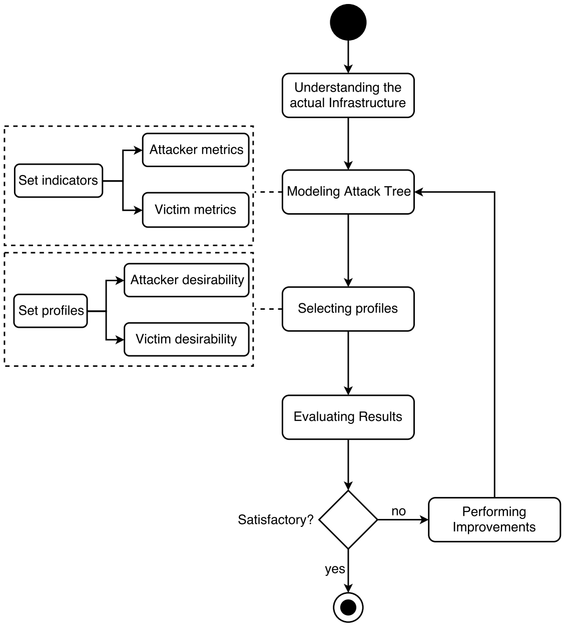


Fig. 3. Strategy for evaluation of an Attack Tree solution

Set indicators (Attacker metrics): the attacker metrics contain reference values for the attacker features, such as behavioral capability (that involves the cost of attack), noticeability, and technical ability.

Set indicators (Victim metrics): the victim metrics contain reference values for the victim features, such as attacker benefits, victim impact for operational losses, and reputation loss.

Selecting profiles: we select profiles, attackers, and victims, after research in literature and biannual reports, with the aim to identify major desirability for the attack and victim countermeasures. After main threats and countermeasure investigation, there is a subprocess with two steps, as described below.

Set profiles (Attacker desirability): the attacker profile provides attacker desires, for example, the spending capability to cause a victim damage and attacker's technical abilities.

Set profiles (Victim desirability:) the victim profile provides victim losses, for example, the capability of operational injuries and reputation loss in cases of attack.

Evaluating results: it evaluates the results generated by attack tree, modeled through the satisfactory condition. If the results are satisfactory, we ended the process. Otherwise, we apply improvements until the model is adequate.

A. DDoS Attack Tree Model

Figure 4 shows a DDoS attack scenario, in which the attacker has full control of the victim's system. The elucidation of each architecture component is presented below: leftmargin=0.18in

- *attacker:* it has full control of the servers connected to networks, labeled as handlers.

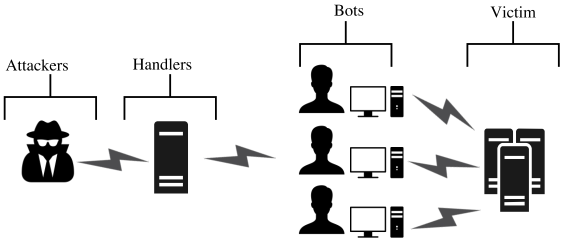


Fig. 4. Possible architecture of a DDoS attack

- *handler:* it represents vulnerable servers connected to the network, with clients everywhere.
- *bots:* it represents vulnerable clients connected to the network, executing illegal tasks in an arbitrary form.
- *victim:* any company connected to internet.

The Attack Tree in Figure 5 was modeled following the architecture of Figure 4. The main DDoS techniques were selected, according to the European Union Agency for Network and Information Security (ENISA) [22].

B. Definition of user and attacker profiles

The Cost of Attack (CoA_i) metrics adopted in the attack tree formalism shown in Equation (3) presents the cost per gate AND, while Equation (4) presents the cost per gate OR. The domain for this equation is $[0, \infty]$ because it cannot be known how much an attacker expects to spend [19].

$$C_{AND} = \sum_{i=1}^{n} CoA_i \tag{3}$$

$$C_{OR} = \frac{\sum_{i=1}^{n} LoO_i \cdot CoA_i}{\sum_{i=1}^{n} LoO_i} \tag{4}$$

Attacker's Benefits (AtB) state the advantages that an attacker will have with a successful attack. It can be calculated by Equation (5). The CoA_i variables used to estimate AtB are given in Table III and in Figure 6(c).

$$AtB = \sum_{i=1}^{n} (CoA_i^2) \tag{5}$$

Feasibility (FeA) metric determines the ease of attack in the evaluated scenario. It is calculated as a geometric mean aiming to compare multiple properties. As exhibited in Equation (6), we adopted CoA_i, Noticeability (NoT_i), and Technical Ability (TeA_i) [20]. The adopted values of these properties are presented in Figure 6.

$$FeA = \sqrt[N]{\prod_{i=1}^{N} CoA_i \cdot NoT_i \cdot TeA_i} \tag{6}$$

Pain Factor (PF) presents the trouble that the victim will undergo if the attack occurs. It is evaluated by how much any attack will harm the target system. It can be calculate

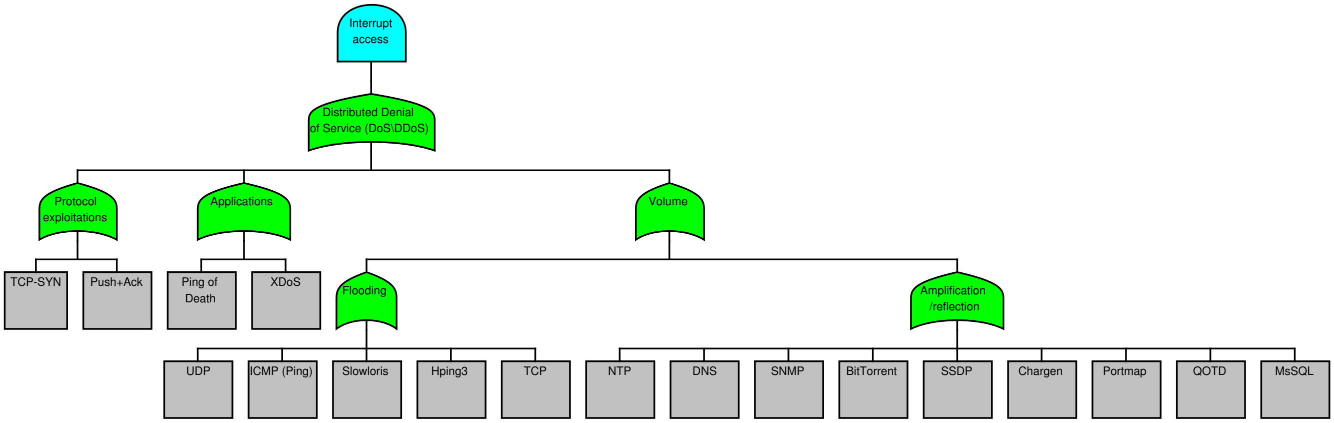


Fig. 5. Model Attack Tree

by Equation (7). To perform such calculations, the values of the Operational Losses (OpL_i) presented in Table III must be obtained through the adoption of OpL_i indicators profiles, whose values are presented in Figure 6(e) [20].

$$PF = \sum_{i=1}^{n} (OpL_i^2) \tag{7}$$

The attack propensity presented in Equation (8) adopts the combination of the feasibility (FeA) and the Attacker's Benefits (AtB) from an attack scenario. The aim is to provide a probability metric of the attack occurrence. This corresponds to the moment in which the agent of the threat hits the target system.

$$AtP = FeA \cdot AtB \tag{8}$$

The Table I shows the used impact descriptions to represent all possible impacts in any system. The danger is also explained on each node and is calculated using the other metrics (see Edge [19]).

TABLE I. Reputation Loss - Victim

Range	$Impact_i$	Impact Definition
$1 \leqslant I < 4$	None	Minor impact on the system.
$4 \leqslant I < 7$	Low	A moderate impact on the system.
$7 \leqslant I < 10$	Medium	Significant damage results to the system.
10	High	The system completely compromised, inoperable, or destroyed.

The Table II enumerates at technical skills of threat agents according to their knowledge level (see Amenaza [23]).

TABLE II. Technical Ability - Attacker

TeA_i	Agent knowledge	Definition knowledge
$20 - 30$	Average user	Can easily surf the Internet, minor knowledge of the system
$30 - 40$	Power user	Low programming skills
$40 - 60$	Advanced user	IT security specialist
$60 - 80+$	God-like status	For all practical reasons, this would be just about impossible

To evaluate the model, we adopted the input parameters presented in Tables I, II, and III. The values used for the node components of the attack tree model (see Section III), the rate of attack per month for each threat, the visibility of each threat against the attacker, the amount of money spent by the attacker to execute the attack and by the victim to protect his infrastructure, and the impact of the threat if it happens were extracted from [24] [25].

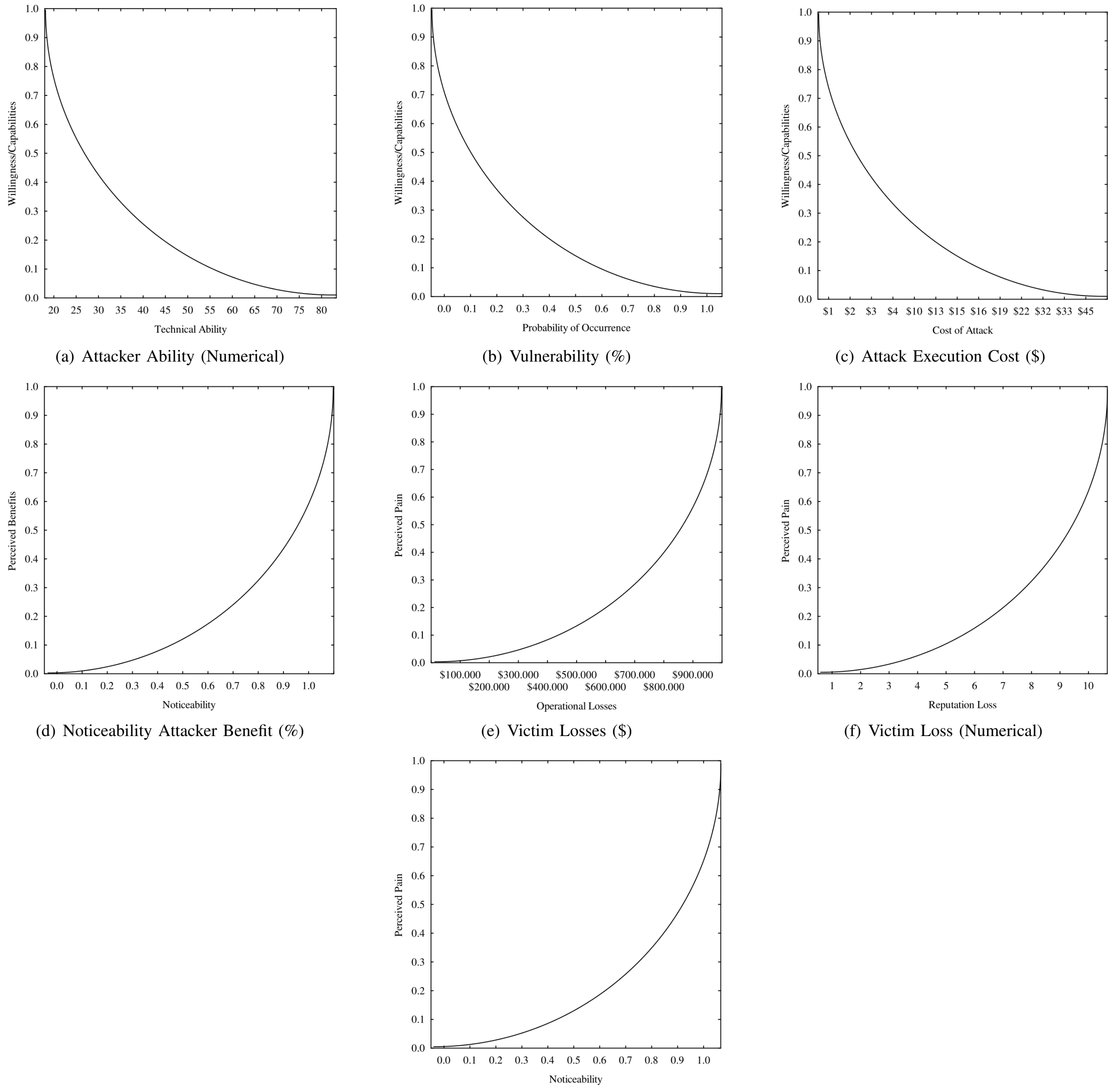
The technical ability indicator is presented in Figure 6(a), which portrays the ability to subvert the evaluated scenario according to the values defined in Table II. The indicator of the probability of occurrence shown in Figure 6(b) represents the relationship between the probability of occurrence and the probability of willingness [26]. Figure 6(c) shows the cost of an attack, which is based on how much an attacker can spend to reach his goal [10]. Figure 6(d) estimates the noticeability of the benefit of the attack to the attacker.

Therefore, the operational losses indicator presented in Figure 6(e), displays the victim's financial losses due to an attack [27]. The losses of reputations in Figure 6(f) arise from the impact of the attack. Table I shows the adverse impact on the victim's reputation [28] [20]. However, the victim noticeability, presented in Figure 6(g) characterizes the victim's visibility with regard to being attacked.

Table III shows the input values for each parameter of the evaluation in the proposed attack tree model. The threats related to $OR\ gates$ (1), (2), (3) and (4) are protocol exploitation, applications, flooding and amplification/reflection respectively. Each gate has a set of leaf nodes that represent the threats.

The scenario was chosen to reach an approximation of the real world. Currently, several companies are adopting safety models for their companies due to their suffering from recurring attacks. In fact, these are happening in various segments whether in the business, educational and/or medical assistance sectors.

In the evaluated context, we propose an attacker's profile as well as his capabilities and a victim's profile in the proposed scenario. The graphics used to draw the profile of an attacker and his capabilities are shown in Figure 6(a). The graph has Y-axis values in percentage, which matches the disposition of the technical ability of an attacker with the scenarios evaluated.



(a) Attacker Ability (Numerical)

(b) Vulnerability (%)

(c) Attack Execution Cost ($)

(d) Noticeability Attacker Benefit (%)

(e) Victim Losses ($)

(f) Victim Loss (Numerical)

(g) Noticeability Victim Impact (%)

Fig. 6. Indicators profiles

The X-axis has the values corresponding to the technical ability of an attacker to submerge in a scenario. This shows that the technical skill of the attacker is given a value of 10.9 and that this value indicates that there is a 50% likelihood of an attack stopping a service. However, as the attacker's technical ability increases, the likelihood of attack decreases.

The proposed profile for the probability of occurrence is shown in Figure 6(b). On the Y-axis, the value is given as a percentage, and the X-axis also matches the percentage. Moreover, it can also be seen that the higher the percentage of the value, the exist the likelihood of the occurrence of an attack.

The profile proposed for the cost of an attack, as shown in Figure 6(c), displays the desire to spend on submerging the service. Note that the Y-axis shows the likelihood that a determined service can be stopped, while the values that the X-axis shows are an expenditure of the attacker. The graph also shows that the attacker is not willing to spend much money to stop a service. For the likelihood of reaching 45% success, the attacker will spend 71.7 dollars. It is remarkable that the

TABLE III. INPUT PARAMETERS REFERENTS OF ATTACK

	CoA_i	LoO_i		OpL_i		NoT_i
$Threats$	($)	(%)	TeA_i	($)	$Impact_i$	(%)
(1) TCP-SYN	2.00	2	10	80.000	None	1
(1) Push+Ack	4.00	4	10	60.000	Low	2
(2) Ping of Death	3.00	4	10	50.000	Low	3
(2) XDoS	1.00	3	20	55.000	None	4
(3) UDP	2.00	40	30	240.000	Medium	2
(3) ICMP	10.00	20	40	140.000	Medium	3
(3) Slowloris	1.00	20	30	220.000	Medium	10
(3) Hping3	1.00	3	40	60.000	Medium	1
(4) TCP	10.00	38	40	205.000	Medium	3
(4) NTP	45.00	51	40	400.000	Medium	20
(4) DNS	32.00	50	60	200.000	High	2
(4) SNMP	19.00	3	60	80.000	Medium	10
(4) BitTorrent	16.00	3	60	90.000	Medium	10
(4) SSDP	15.00	37	50	340.000	High	4
(4) Chargen	33.00	7	60	90.000	Medium	3
(4) Portmap	22.00	5	50	90.000	Low	4
(4) QODT	13.00	3	60	130.000	Medium	1
(4) MsSQL	10.00	20	40	400.000	Medium	3

profile of this attacker is at a low level.

Figure 6(d) shows the visibility indicator of the benefits of the attacker. We observed values related to the probabilities of the attacker gaining benefits from the attack. For example, when there is an 80% probability, the benefit from the attack will be 100%.

Figure 6(e) shows the indicator linked to the operating losses of the victim, with the occurrence of the attacks. The Y-axis shows values relative to the percentages of the victims occurrences of loss. For example, when there is a 40% probability, the loss of operating income will be $900,000. Moreover, 6(f) shows the indicator linked to the company's reputation, by ranking given in Table I, which shows that the higher the value on the Y-axis, the more likely it is that the company will suffer the loss of reputation. For example, with 40% probability, the victim's reputation will drop from 10th to 1st position in the ranking, However, 6(g) gives evidence that the indicator that accounts for the visibility of the victim, shows that the higher the probability on the Y-axis, the higher is the chance of the victim being exposed to the attack. For example, with a 60% probability, the victim is 100% exposed to the attack.

IV. RESULT ANALYSIS

Given the proposed scenario and the evaluated model, we obtained results for the Likelihood of attack, Cost of attack, Attacker's benefits, Feasibility, Pain factor, Propensity of attack and Technical ability. Figure 7 shows the attack occurrence probability for the most probable methods. Y-axis shows the attack level as a percentage likelihood, while X-axis identifies the possible scenarios that can be subverted. The amplification technique has a 94% chance of occurrence. The second most likely form of attack would use the Flooding technique and had a 63% chance of occurrence; the third with a 90% likelihood of occurrence was the Applications technique, and the fourth with a 60% chance of occurrence was the Protocol Exploration technique. According to depicted results, the Amplification technique is 31% more probable to occur than the flooding technique.

Results regarding Cost of Attack are presented in Figure 8. The primary attacker method is also Amplification. In the second place, the Flooding method, followed by the Protocol method, and in fourth place, the Application method. With such a ranking, the security analyst will be aware of the most significant threats and will be able to direct efforts to tackle them. In the evaluated context, it is observed that the attacker has to invest 28 dollars to reach his goal. However, he spends 4 dollars using the Flooding method, 3 dollars on the Protocol method, and 2 dollars using the Application method. These values refer mainly to the cost of hardware, software, and bandwidth for stopping the service.

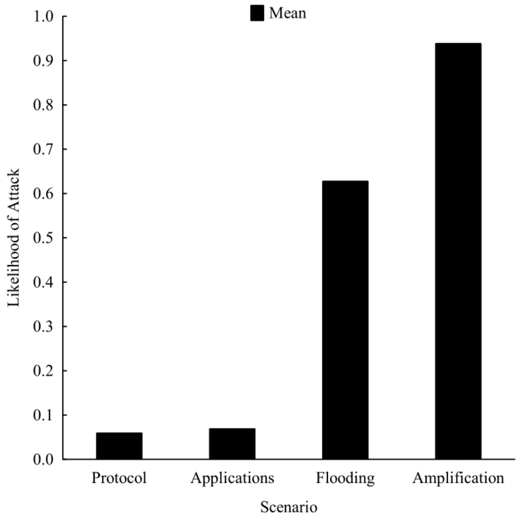


Fig. 7. Likelihood of Attack

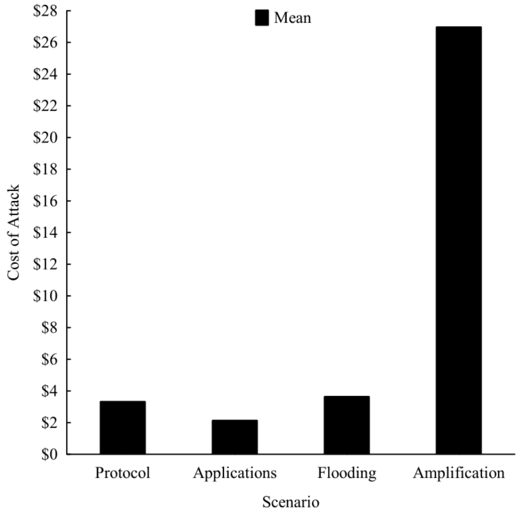


Fig. 8. Cost of Attack

Figure 9 depicts the possible gains of invasion for the main threats. The primary attacked service is NTP, in second place, Slowloris, SNMP, and BitTorrent, followed by to SSDP and Portmap services. These are the main threats that the security analyst will have to pay most attention and devote most effort. The attacker will have a 10% chance of obtaining benefits using the NTP attack, while as a result of using the Slowloris, SNMP and BitTorrent, methods, he will have a 5% probability of obtaining benefits.

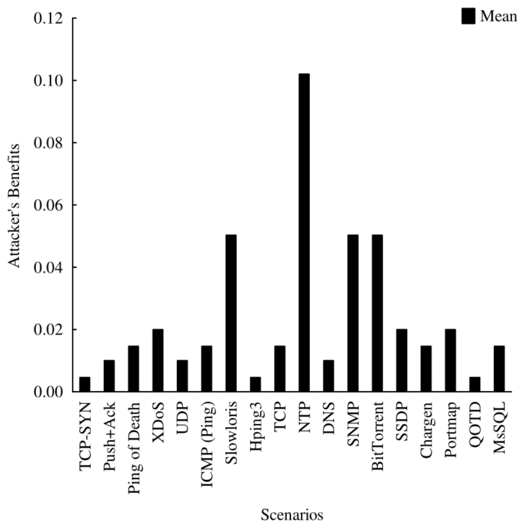


Fig. 9. Attacker's Benefits

Figure 10 shows the easiest attack techniques. The TCP-SYN has an 80% chance of occurrence, followed by Hping3, with 70% probability of occurrence.

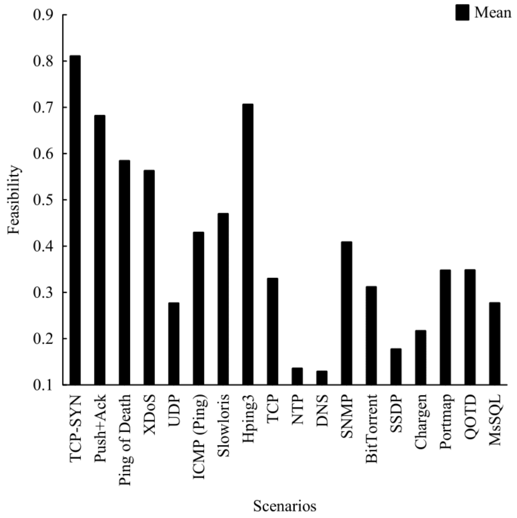


Fig. 10. Feasibility

Figure 11 illustrates companies pain factor due to attack occurrences. In the evaluated context, the pain factor involves several factors that are prejudicial to companies, namely operational, financial, and reputation losses. The threats ranked in descending order in this Figure were found to have the following likelihood of occurrence: the NTP attack method 5%, the MsSQL method 4.7%; and SSDP 4.3%.

Figure 12 shows the methods of attack that are most likely to occur. Several factors contribute to this result, such as the technical ability of the attacker, the perception of threats, the cost of the attack, the ease of attack and the benefits from the attack. Given this, we obtained the propensity for attacks to occur. We observed the threats that are most likely to occur given the set of characteristics. As it has a 2.3% occurrence, Slowloris has the highest propensity, followed by SNMP with a 2.1% probability and the BitTorrent technique had a 16% chance of occurring.

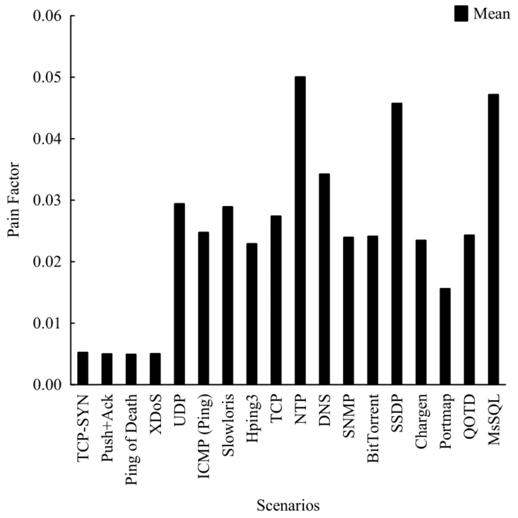


Fig. 11. Pain Factor

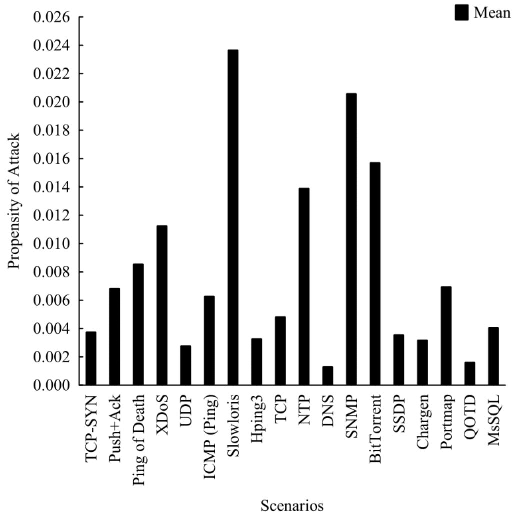


Fig. 12. Propensity of Attack

Figure 13 shows the technical skills required by the attacker to perform an attack. Knowing the invader skills can reduce the attack effects. As can be observed, the two most knowing technical abilities of the attacker are TCP-SYN technique, with 72% of knowledge to subvert the system, and Push+Ack technique, with 60% of knowledge.

The evaluated results show values referring to the attack occurrence probability, from the both attacker's and victim's point of view. The relevance of these results shows us which techniques can be used in analyzed context. Therefore, the victim can make individual decisions regarding the threat. The study addresses only attack-oriented threats from attacks of distributed denial-of-service (DDoS). Moreover, the attack tree can be used to model any threat risk analysis.

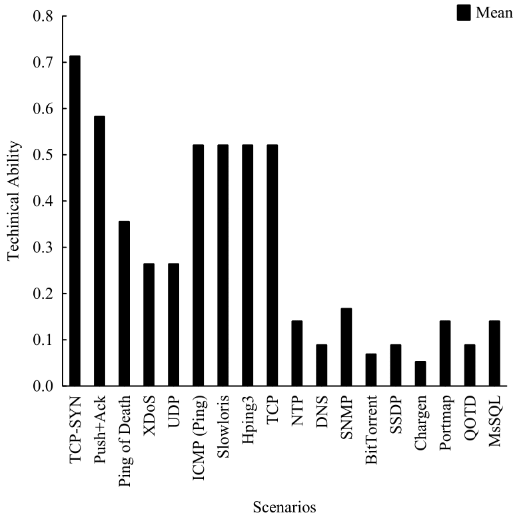


Fig. 13. Technical Ability

V. Final Remarks

This paper described an analytical-based approach to evaluate the impact of distributed denial-of-service attacks directed to a computer system. An attack tree simulation model was proposed as an evaluation approach to obtain the results for several metrics of interest, as well as the benefits of the solution, by measuring and adjusting specific computing components for the analytical solution and the simulation models.

The obtained results showed that the techniques of distributed denial-of-service attack impacted the victim significantly. The attack occurrence likelihood is 95.8% using amplification techniques. Also, there is a feasibility of 82.1% on using the TCP+SYN technique and 71.0% using the Hping3 technique. Another evaluated metrics are the pain factor, which has a 5.1% probability of occurrence and the propensity of attack, with 2.4% chance of happening.

In a future study, we intend to use attack tree models to evaluate the impact of virtual and physical attacks in cloud computing infrastructures, by using metrics of multivariate analysis, such as the likelihood of attack, cost of attack, attacker benefits, the propensity of attack and feasibility. Also, trend and time-series analysis may be used as means to prevent and mitigate the impact of DDoS attacks.

References

[1] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[2] P. Wood, B. Nahorney, K. Chandrasekar, S. Wallace, and K. Haley, "Internet security threat report," *Symantec*, vol. 17, 2016.

[3] D. Dyn, "Large ddos attacks cause outages at twitter spotify and other sites," https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/, accessed: 2017-02-01.

[4] C. C. Center, "Cert advisory ca-1998-01 smurf ip denial-of-service attacks," 1998.

[5] Neustar, "Worldwide ddos attacks e cyber insights research report," *A Neustar Security Solutions Exclusive*, pp. 1–52, 2017. [Online]. Available: https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/neustar-2017-worldwide-ddos-attacks-cyber-insights-research-report.pdf

[6] C. Isaca, "Review manual 2011," *Information Systems Audit and Control Association Inc., ZDA*, 2010.

[7] Protiviti, "Internal audit capabilities and needs survey," *Protiviti*, pp. 1–42, 2017. [Online]. Available: https://www.protiviti.com/sites/default/files/united_states/insights/2017-internal-audit-capabilities-and-needs-survey-protiviti.pdf

[8] A. Roy, "Attack countermeasure trees: A non-state-space approach towards analyzing security and finding optimal countermeasure sets," Ph.D. dissertation, Duke University, 2010.

[9] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *Icisc*, vol. 3935. Springer, 2005, pp. 186–198.

[10] B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21–29, 1999.

[11] K. S. Edge, *A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees*. Air Force Institute of Technology, 2007.

[12] N. author, "More nsa revelations: backdoors, snooping tools and worldwide reactions," *Network Security*, vol. 2014, no. 1, pp. 1 – 20, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485814700017

[13] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets." *SRUTI*, vol. 5, pp. 6–6, 2005.

[14] T. OWASP, "10 2010," *The Ten Most Critical Web Application Security Risks*, vol. 30, 2010.

[15] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," *ACM SIGCOMM Computer Communication Review*, vol. 19, no. 2, pp. 32–48, 1989.

[16] W. M. Eddy, "Tcp syn flooding attacks and common mitigations," *IETF Trust*, 2007.

[17] B. CERT, "Centro de estudos, respostas e tratamento de incidentes de segurança no brasil."

[18] P. Suhasaria, A. Garg, A. Agarwal, and K. Selvakumar, "Distributed denial of service attacks: A survey," *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 2, 2017.

[19] K. S. Edge, G. C. Dalton, R. A. Raines, and R. F. Mills, "Using attack and protection trees to analyze threats and defenses to homeland security," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*. IEEE, 2006, pp. 1–7.

[20] T. R. Ingoldsby, "Attack tree-based threat risk analysis," *Amenaza Technologies Limited*, pp. 3–9, 2010.

[21] T. Isograph, "Attack tree," *Isograph*, 2017. [Online]. Available: https://www.isograph.com/software/attacktree/

[22] C. Lévy-Bencheton, L. Marinos, R. Mattioli, T. King, C. Dietzel, and J. Stumpf, "Threat landscape and good practice guide for internet infrastructure," *Report, European Union Agency for Network and Information Security (ENISA)*, 2015.

[23] T. R. Ingoldsby, "Amenaza demos," *Amenaza Technologies Limited*, 2010. [Online]. Available: https://www.amenaza.com/demos/introduction_to_securitree.html

[24] A. Networks, "Worldwide infrastructure security report," *Network Security*, pp. 1–104, 2017. [Online]. Available: https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf

[25] C. C. ENISA, "Benefits, risks and recommendations for information security," *European Network and Information Security*, 2009.

[26] D. Ren, S. Du, and H. Zhu, "A novel attack tree based risk assessment approach for location privacy preservation in the vanets," in *Communications (ICC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1–5.

[27] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[28] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, p. 1, 2009.