2018 IEEE International Conference on Systems, Man, and Cybernetics

Impact Assessment of Multi-threats in Computer Systems Using Attack Tree Modeling

Ronierison Maciel*, Jean Araujo†‡, Carlos Melo*, Jamilson Dantas*, and Paulo Maciel*
*Centro de Informática, Universidade Federal de Pernambuco, Recife, Brazil
†Unidade Acadêmica de Garanhuns, Universidade Federal Rural de Pernambuco, Garanhuns, Brazil
‡NOVA LINCS & DI, FCT, Universidade NOVA de Lisboa, Caparica, Portugal
{rsm4, casm3, jrd, 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 and malicious software in computer systems. We propose hierarchical models that represent the behavior of major system components and assess the effects of a DDoS and Malware attack on the system availability. We also 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 attack tree indices show the impact of simultaneous attacks on a computer system and the several threats which will maximize the system downtime. The results obtained from the attack tree analysis allow to plan and improve system's availability, maintainability, and reliability.**

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

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] and Malicious Software (Malware) [3]. At the early of 2018, GitHub faced catastrophic events [4]. A DDoS attack of 1.35 terabits per second of traffic hit the developer platform, that were inaccessible for eight minutes.

The DDoS method came to notice in 1997 [5], but computer virus concept was defined early in 1986 [6] as a program that can infect other programs. 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. 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 malware [7]. It was extremely alarming, as the remaining 93% of companies are subject to catastrophic corruption by virtual threats. Malicious activities result in losses for enterprises, data centers management, health systems, and real-time operating systems. 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 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 and Malware 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 security threats, 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 security threats, with focus on DDoS and Malware attacks, and basic concepts of attack tree modeling.

A. Security Threats

Computational threats impact in operational losses and another aspect. The main risks that impact are:

- *Backdoor:* the attacker connect to the computer with little or no authentication and execute commands

2577-1655/18/$31.00 ©2018 IEEE
DOI 10.1109/SMC.2018.00420

- *Botnet:* but all computers infected with the same botnet receive the same instructions from a single command-and-control server.

An application layer DDoS attack 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 [12]. 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 .Backdoor is a malicious software that infects the victim and provides full access to the user's computer and its resources. 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].

Besides, malicious software (or malware) performs a part in most computer intrusion and security incidents. Any software that does something that causes harm to a user, computer, or network can be considered malware, including viruses, trojan horses, worms, rootkits, scareware, and spyware [3]. Backdoor Malicious code that auto-install itself into the victims' computers to allow the attacker access. However, backdoors usually let the attacker connect to the network with little or no authentication and execute commands on the local system [14]. A malware may collect data and information from victims' computer and transfers typically it to the attacker [15], and can be used to gain access to online accounts such as email or online banking; examples include sniffers, password hash grabbers, and keyloggers.

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) is an emerging and promising approach that aims to reduce financial losses by mitigating threats [16]. 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 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. 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 [17].

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

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

There are tools that can automate the whole process of threat investigating through the adoption of ATs [18]. 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.

III. Proposed Model

This section presents the proposed model to analyze the primary DDoS and Malware 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 needs to define a list of leading 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 1 shows a DDoS and Malware attack scenario, in which the attacker has full control of the victim's system. Each architecture component is presented below:

- *Access by threats:* virtual threats infect users, labeled as malware, dashed line of red.
- *Access by super-user:* it represents access by super-user connected to the network, dashed line of blue.
- *Victim:* any company connected to the internet dashed line of green.

The Attack Tree in Figure 2 was modeled following the architecture of Figure 1. The main DDoS techniques were selected, according to the European Union Agency for Network and Information Security (ENISA) [19].

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 [17].

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

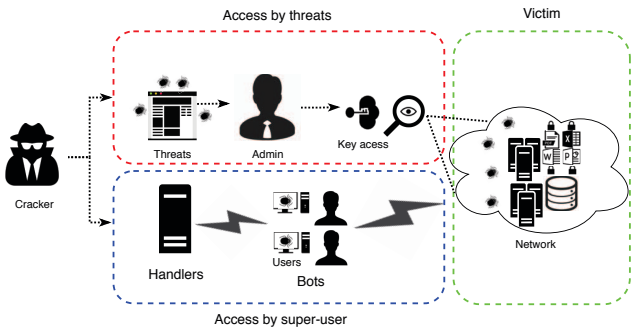


Fig. 1. The possible architecture of an attacker

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

Attacker's Benefits (AtB) state the advantages that an attacker will have with a successful attack. It can be calculated by Equation (5). The W_i weighting and P_i likelihood variables used to estimate AtB are given in Table III and in Figure 3(c).

$$AtB = \sum_{i=1}^{n} (W_i \cdot P_i) \tag{5}$$

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) [18]. The adopted values of these properties are presented in Figure 3.

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

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 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 3(e) [18].

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

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. They correspond to the moment in which the agent of the threat hits the target system.

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

In the evaluated context, we propose an attacker's profile as well as his capabilities and a victim's profile in the proposed scenario. Figure 3 shows the indicators profiles.

The graphics used to draw the profile of an attacker and his capabilities are shown in Figure 3(a). The graph has Y-axis values in percentage, which matches the disposition of the technical ability of an attacker with the scenarios evaluated. 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 3(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 (see Figure 3(c)) shows 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.

Figure 3(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 victim's occurrences of loss. Moreover, 3(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. However, 3(d) gives evidence that the indicator that accounts for the visibility of the victim, and shows that as higher is the probability on the Y-axis, higher is the chance of the victim being exposed to the attack.

IV. Case Study

The case study 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.

A. Input Parameters

To evaluate the proposed 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, 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 [20] [21].

Table I shows the used impact descriptions to represent all possible impacts in any system [17].

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.

Table II enumerates at technical skills of threat agents according to their knowledge level [22].

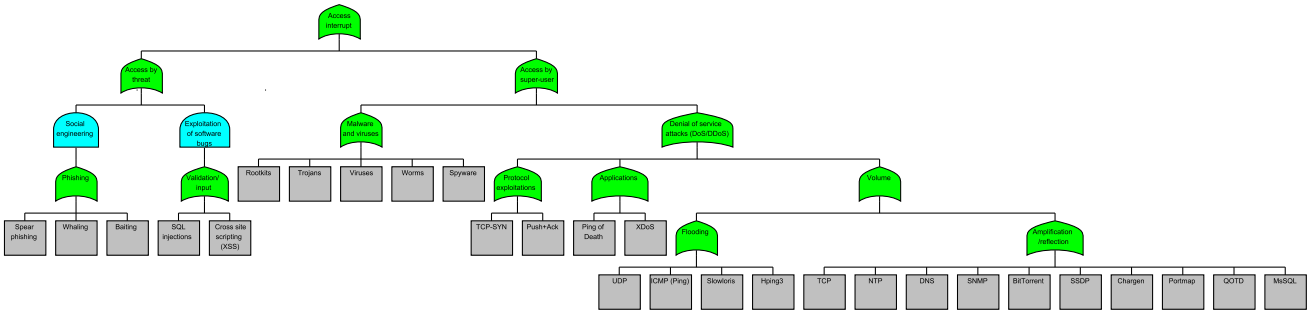
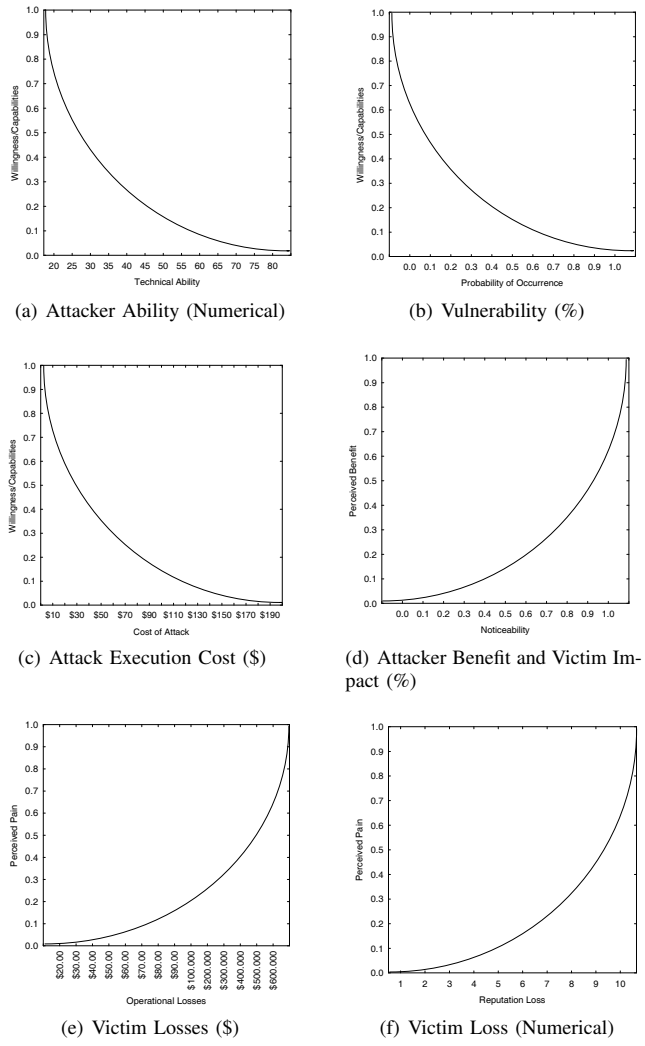


Fig. 2. Model Attack Tree



(a) Attacker Ability (Numerical)

(b) Vulnerability (%)

(c) Attack Execution Cost ($)

(d) Attacker Benefit and Victim Impact (%)

(e) Victim Losses ($)

(f) Victim Loss (Numerical)

Fig. 3. Indicators profiles

The threats in Table III related to OR gates are access by threats or super-user. Besides, AND gates social engineering and software bug exploitation. However, others gates we can see in Figure 2.

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

TABLE III. INPUT PARAMETERS REFERENTS OF ATTACK

$Threats$	CoA_i ($)	LoO_i (%)	TeA_i	OpL_i ($)	$Impact_i$	NoT_i (%)
Spear phishing	200.00	10	80	400.000	High	10
Whaling	200.00	10	80	500.000	High	10
Baiting	200.00	12	60	300.000	Medium	12
SQL injection	60.00	12	40	140.000	Medium	12
XSS	60.00	1	40	150.000	Medium	3
Rootkits	60.00	1	80	300.000	Medium	3
Trojans	60.00	20	60	200.000	Medium	10
Viruses	60.00	10	60	150.000	Medium	10
Worms	60.00	10	60	150.000	Medium	10
Spyware	60.00	10	60	110.000	Medium	4
TCP-SYN	60.00	2	10	80.000	None	1
Push+Ack	60.00	4	10	60.000	None	2
Ping of Death	60.00	4	10	50.000	None	3
XDoS	100.00	3	60	55.000	Medium	4
UDP	60.00	40	30	240.000	High	2
ICMP (Ping)	60.00	20	10	80.000	Low	3
Slowloris	60.00	20	40	70.000	Medium	10
Hping3	60.00	30	40	70.000	Low	1
TCP	60.00	38	40	205.000	Medium	3
NTP	100.00	51	80	600.000	High	20
DNS	100.00	50	60	300.000	High	2
SNMP	60.00	3	30	120.000	High	10
BitTorrent	60.00	20	80	250.000	High	10
SSDP	60.00	37	50	340.000	High	4
Chargen	100.00	7	40	80.000	Medium	3
Portmap	60.00	5	40	90.000	Medium	4
QODT	60.00	3	40	100.000	Medium	1
MsSQL	60.00	10	80	200.000	Medium	3

B. 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 4 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 67% chance of occurrence; the third with a 43% likelihood of occurrence was the Malware technique, and the fourth with a 25% chance of occurrence was the Phishing technique. According to depicted results, the Amplification technique is

17% more probable to occur than the Validation technique.

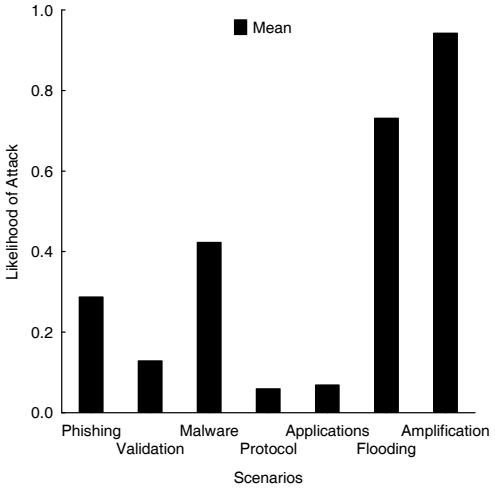


Fig. 4. Likelihood of Attack

Results regarding Cost of Attack are presented in Figure 5. The primary attacker method is also Phishing. In the second place, the Amplification method, followed by the Applications method, and in fourth place, the Validation, Malware, Protocol, and Flooding 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 220 dollars to reach his goal. However, he spends 220 dollars using the Phishing method, 80 dollars on the Amplification method, and 77 dollars using the Applications method. These values refer mainly to the cost of hardware, software malicious, and bandwidth for stopping the service.

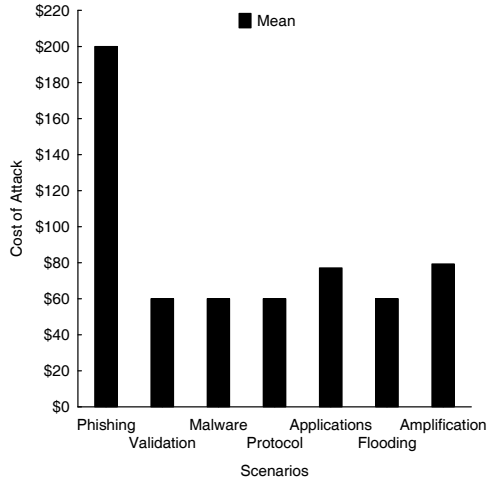


Fig. 5. Cost of Attack

Figure 6 shows the easiest attack techniques. The TCP-SYN has a 63% chance of occurrence, followed by SQL injection, with 60% probability of occurrence.

Figure 6 illustrates companies pain factor due to attack occurrences. In the evaluated context, the pain factor involves

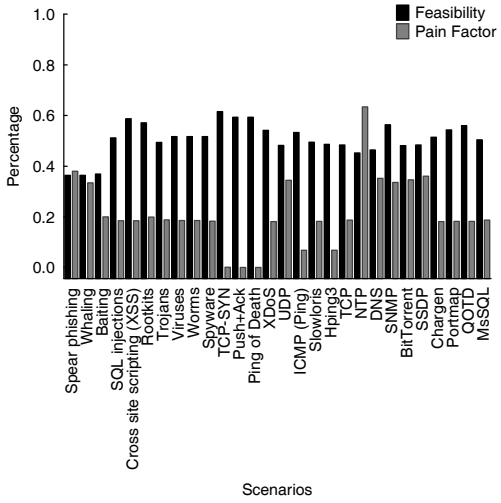


Fig. 6. Feasibility and Pain Factor

several factors that are prejudicial to companies, namely operational, financial, and reputation losses. The threats ranked in descending order were found to have the following likelihood of occurrence: the NTP attack method 67%, the Spear phishing method 39%; and SSDP 37%.

Figure 7 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 0.7% occurrence, NTP has the highest propensity, followed by SQL injection with a 0.3% probability and the Slowloris technique had a 0.2% chance of occurring.

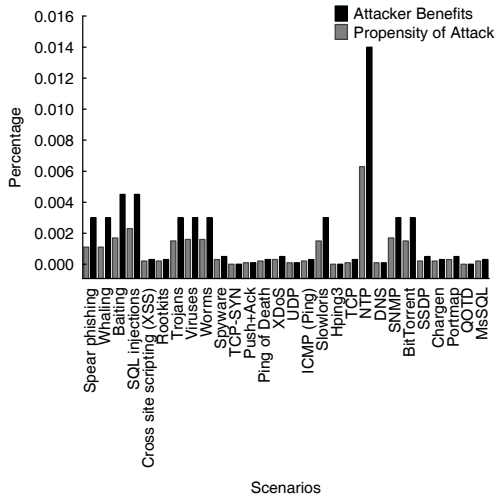


Fig. 7. Attacker Benefits and Propensity of Attack

Figure 7 depicts the possible gains of invasion for the main threats. The primary attacked service is NTP, in second place, Baiting, and SQL injection, followed by to Trojans, Viruses,

and Worms. These are the main threats that the security analyst will have to pay most attention and devote most effort. The attacker will have a 1.4% chance of obtaining benefits using the NTP attack, while as a result of using the Baiting, and SQL injection, methods, he will have a 5% probability of obtaining benefits.

Figure 8 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, Push+Ack, and Ping of Death, technique, with 90% of knowledge to subvert the system, and SNMP technique, with 70% of knowledge.

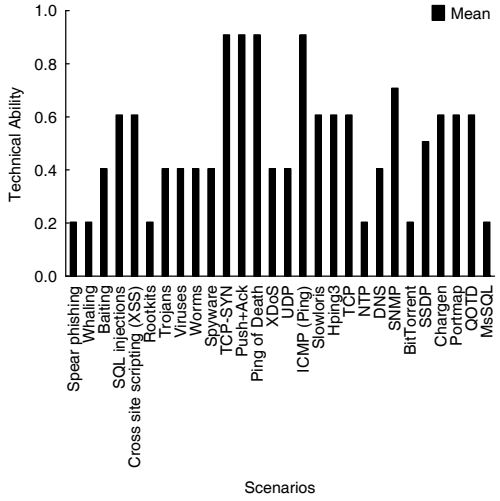


Fig. 8. Technical Ability

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) and Malware. Moreover, the attack tree can be used to model any threat risk analysis.

V. Final Remarks

This paper described an analytical-based approach to evaluate the impact of distributed denial-of-service attacks and malicious software 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 and malware attack impacted the victim significantly. The attack occurrence likelihood is 95.8% using amplification techniques and 75.2% flooding technique. Also, there is the feasibility of 62.1% on using the TCP+SYN technique and 58.0% using the Hping3 technique. Another evaluated metrics are the pain factor, which has a 1.2% probability of occurrence and the propensity of attack, with 0.1% 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] M. Sikorski and A. Honig, *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press, 2012.

[4] L. Newman, "Github survived the biggest ddos attack ever recorded," https://www.wired.com/story/github-ddos-memcached/, accessed: 2018-02-02.

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

[6] F. Cohen, "Computer viruses: theory and experiments," *Computers & security*, vol. 6, no. 1, pp. 22–35, 1987.

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

[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. Dobb's 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] T. OWASP, "10 2010," *The Ten Most Critical Web Application Security Risks*, vol. 30, 2010.

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

[14] K. Rieck, T. Holz, C. Willems, P. Düssel, and P. Laskov, "Learning and classification of malware behavior," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2008, pp. 108–125.

[15] E. Skoudis and L. Zeltser, *Malware: Fighting malicious code*. Prentice Hall Professional, 2004.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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

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

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