Framework for evaluating Capture The Flag (CTF) security competitions

Raghu Raman[1], Sherin Sunny[2], Vipin Pavithran[2]

, Krishnasree Achuthan[2]

[1] Center for Research in Advanced Technologies for Education
Amrita University, India
{ raghu@amrita.edu }

[2] Amrita Center for Cyber Security
Amrita Vishwa Vidyapeetham, Amritapuri, Kollam – 690525
{ sherin081991@gmail.com , vipinp@am.amrita.edu, krishna@amrita.edu }

***Abstract*— A large number of ethical hacking competitions are organized worldwide as Capture The Flag (CTF) events. But there does not exist a framework to evaluate and rank CTFs that will guide participants as to which CTF's to participate. In a CTF event, the participants are required to either solve a set of challenges to gain points or they are required to defend their system by eliminating the vulnerabilities while attacking other's system vulnerabilities. We are proposing a framework that would evaluate and rank CTFs according to factors like similarity of the tasks to the common critical vulnerabilities, solvability of tasks, periodicity, training given prior to CTF, geographical reach, problem solving skills etc. In the next step these factors are systematically assigned weights using Analytic Hierarchy Process. As part of frame work creation and validation, ten CTFs have been analysed. Our analysis indicates that: All CTFs fall in to one of the three categories (jeopardy, attack-defence and mixed); CTFs often adopt popular software vulnerabilities and threats as tasks to be solved; Only few CTFs give formal training prior to the event; Complexity of the tasks to be solved varies from CTF to CTF. Five CTFs were ranked using the newly developed framework.**

***Keywords*— CTF, Analytic Hierarchy Process, Framework, Hacking, Vulnerability**

I. INTRODUCTION

With the extensive use of internet, the world is increasingly relying upon on cyber infrastructure. Criminals and hackers make use of this environment in a better way than protectors [1,2]. Hence there exist a crucial need to safeguard security and privacy of applications and systems. With a view of imparting training to students in the field of cyber security, ethical hacking competitions are conducted worldwide.

Capture The Flag (CTF) is the best known ethical hacking competition in the hacker community. In CTF, the participants are required to either solve a set of tasks or they are required to defend their system by eliminating the vulnerabilities while attacking other's systems. Since CTFs are usually run by security experts, it has become an emerging criterion for cyber security education and research [3].Although there are three different formats for organizing CTF namely jeopardy, attack-defence and mixed, most of the CTF contests adopt jeopardy style [4].Jeopardy style CTF has a series of tasks to be solved or answered whereas attack-defence style CTF provides a system with a set of vulnerable services that are supposed to be eliminated , at the same time attacking other's systems.

Though large number of ethical hacking competition is organized as CTF Worldwide, there does not exist any framework to evaluate CTFs and rank them accordingly. This paper addresses the development of framework that would evaluate and rank CTF according to certain defined factors called framework. Once the CTFs are rated with respect to a framework, the quality of CTFs gets uplifted. Participation in better rated CTFs helps the competitors to advertise their capabilities to prospective researchers and employers. It also helps the organizers who are new to CTF contest to conduct superior CTFs by analysing the framework. Moreover, Cyber security education can be standardized by mapping the expertise they acquire by participating in CTFs with that of the required skills.

.

II. THEORETICAL BACKGROUND

For the purpose of testing a participant's problem solving skills, CTF contests are organized by incorporating innovations along with entertainment [3].Due to the extreme shortage of talented security professionals, there exists a critical need of holding CTFs [5].CTF act as a good platform to gain knowledge and skills based on cyber security [6].

Hacking competitions help the students to get exposed to real time scenarios. Here, students can gain hands on experience by participating in CTF events. The skills acquired while participating in CTFs are essentially useful, as recruiters often look for such skill set in their prospective employees [7]. Nevertheless, there are students who lack the necessary skills required for participating in hacking contest. Only few CTFs such as InCTF and MIT LL educate and train participants prior to the contest. They offer several sessions and lab tests based on CTF so that students with inadequate skills can have adequate practice which will enable them to perform successfully [9]. As part of the training, students could study

Authorized licensed use limited to: University of Zagreb. Downloaded on October 18,2024 at 15:08:26 UTC from IEEE Xplore. Restrictions apply.
978-1-4799-3759-2/14/$31.00©2014 IEEE

the code, system vulnerabilities and methods of overcoming the vulnerabilities. They can learn methods of developing scripts to secure their systems and explore other's [10]. The most challenging part in holding cyber security exercise is to create the critical set of vulnerable services. It is essential to keep services moderately complex [10,11].

In order to have a strong national cyber infrastructure that encompasses talented security professionals, it is essential to create awareness about cyber security careers. As an initiative to create this awareness and to monitor and encourage the development of US cyber security competitions, Department of Homeland Security has a launched Cyber Competitions Project (CCP) [12]. With a view to create awareness among the citizens regarding cyber security, India's national cyber security policy has also initiated some awareness programs, cyber security workshops and seminars. It urges public and private organizations to work hand in hand in defending cyber threats .The policy also promotes research in the field of cyber security in collaboration with industries and academia [13]. It is also advised to incorporate cyber security as part of the academic curriculum of students of all levels [14].

Most of the security breaches occur due to lack of security awareness. It is necessary to include security education as part of undergraduate curriculum [15].It is not always essential to have sophisticated set up to hold cyber security exercise. Even a single faculty member can run several small scale cyber security exercises in a variety of formats [16]. However, hosting a large scale hacking competition is rather time consuming and challenging [11].

DEF CON CTF is the biggest oldest and highly publicized hacking contest. UCSB iCTF is one of the largest academic CTF competitions [17]. Students participating in CTFs are found to have a deep understanding on various security aspects. Also CTF provide a good platform for the students to interact with the hacker community [18].A drawback of CTF contests is that the game is organized for a limited duration. This helps participants to use common methods and strategies. It is noticed that most of the CTF contests do not address availability issues of real life scenarios [19].

III. DATA COLLECTION AND ANALYSIS

As part of the research study, ten CTFs have been analyzed (Table 1).

TABLE I
DESCRIPTION OF CTF CONTESTS

CTF contest	**DESCRIPTION**
DEF CON CTF	Jeopardy for first round and attack-defence format for final round, good incentives and recognition offered, team size limited to 8, Challenges :-[SQL injection, cross site scripting, buffer overflow, timing attacks , heat exploits, malformed network constructs etc.], 898 teams in DEF CON 2012, 2 rounds, qualification online and final onsite, Held yearly, International. Official URL: http://ddtek.biz/
UCSB Ictf	Attack-defence format, good incentives and recognition, no team size limitation, Challenges: [Deobfuscation, binary, web, application security, network security, reverse engineering, buffer overflow etc], 71 teams participated in iCTF 2012, 1 round, Online, Held yearly, International. Official URL: http://ictf.cs.ucsb.edu/
3.Mozilla CTF	Jeopardy format, good incentives, no team size limitation, Challenges:-[Exploitation, crypto, cracking, web security etc], 49 teams participated in Mozilla CTF 2012, 1 round, Online, Held once, International. Official URL: https://wiki.mozilla.org/Security/Events/CTF
PHD CTF	Jeopardy for first round and attack-defence format for final round, good incentives, team size limited to 7, Challenges:-[Attack other team's services and get flags. Solve the tasks. Keep their own services running.], 154 teams participated in PHD CTF 2012, 2 rounds, qualification online and final onsite. Held yearly, International. Official URL: http://quals.phdays.ru/
RuCTFe	Attack-defence format, good incentives offered, no team size limitation, Challenges: [SQL injection, binary exploitation, buffer overflow, reverse engineering, buffer overflow etc.], 82 teams participated in RuCTFe 2012, 1 round, Online, Held yearly, International .Official URL: http://ructf.org/e/
Hack.lu CTF	Jeopardy for first round and attack-defence format for final round, good incentives offered, no team size limitation, Challenges:-[Crypto, reverse engineering, forensics, web security etc], 260 teams participated in Hack.lu 2012, 1 round, Online, Held yearly, International. Official URL: http://hack.lu/
SECUINSI-DE CTF	Jeopardy format, good incentives, team size limited to 8, Challenges:-[Crypto, reverse engineering, forensics, web security], 259 teams participated in SECUINSIDE CTF 2013, Conducted online, Held yearly, International. Official URL: http://ctf.secuinside.com/
rwth CTF	Attack-defence format, good incentives offered, no team size limitation, Challenges:-[Binary exploitation challenge, android cell phone challenge, cryptographic challenge, code war games etc], 76 teams participated rwth CTF 2012, 1 round, conducted online. Held yearly, International. Official URL: http://ctf.itsec.rwth-aachen.de/
CSAW CTF	Jeopardy for first round and attack-defence format for final round, good incentives and recognition offered, no team size limitation, Challenges:-[Trivia , Recon, Web, reversing, exploitation, miscellaneous, crypto, etc], 1380 teams participated, qualification online and final onsite, Held yearly, International. Official URL: https://ctf.isis.poly.edu/
PICO CTF	Jeopardy format, good incentives offered, team size limited to 8, Challenges:-[Crypto, reverse engineering, forensics, web security, etc], 1938 teams participated, Conducted online, Held yearly, International. Official URL: https://picoctf.com/

Authorized licensed use limited to: University of Zagreb. Downloaded on October 18,2024 at 15:08:26 UTC from IEEE Xplore. Restrictions apply.

A. Performance of various CTFs

Difficulty level of a CTF can be mapped in to solvability of tasks. Fig. 1 displays variation in the percentage of tasks solved with respect to participated teams. Higher the percentage of participated teams, higher the percentage of solved tasks, easier the CTF is.

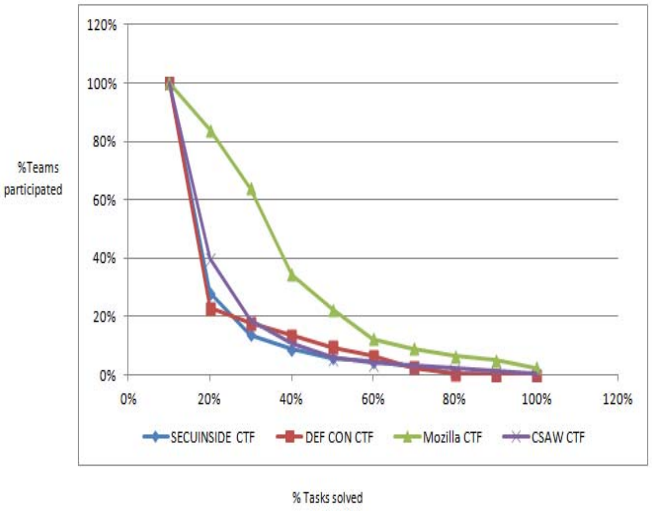

Fig. 1 Graph showing performance of various CTFs

IV. Construction of Framework by Defining Factors

A framework to gauge the relative importance of the factors tested in CTFs is developed by identifying the ten most important factors as detailed below. Weights are assigned to each of them and all the CTFs are examined against each of these factors. Points are then awarded after analyzing CTFs against each factor. Rating is based on cumulative sum of points corresponding to the weight of each factor. The factors are elaborated in the following sections.

A. Challenge classification and mapping (vuln)

The CTF contests are first classified based on the types of challenges they cover. These categories are then mapped to well-known software development vulnerabilities and OWASP vulnerabilities (vuln). Weightage is given to the breadth of vulnerabilities covered. Higher the coverage within the CTF, larger is the points. The well-known OWASP vulnerabilities include injection flaws, buffer overflow, cross site scripting, cross site request forgery, OS commanding, remote file inclusion, path traversal etc.

B. Solvability of the tasks

This framework defines solvability as the percentage of participants that are able to solve a certain percent of the problems. As an e.g. a certain of questions in a contest could be solved by a handful of participants. On the other hand, there may be select problems that are only solved by a handful of participants .This solvability factor is directly proportional to the difficulty rating of the CTF. The framework looks at this spectrum of variation for all problems within CTF. The difficulty level increases with decrease in the percentage of participants attempting and successfully solving problems.

C. . Ratio of 'difficulty level' of the task to the 'solved ratio' (ratio)

To normalize results, the difficulty levels are perceived as a function of the number of the solved tasks. In contrast, easy CTFs produce problems that may be easily solved.

D. Periodicity of CTFs (periodic)

The framework considers the yearly periodicity of the CTF as a factor that affects the publicity and therefore participation in the event. As an e.g. DEF CON CTF is one of the oldest CTFs that began in 1996. Today it continues to remain as one of the most coveted events from a cyber security contest perspective. Also the higher the periodicity, the CTF organizers would have a more refined, established gaming architecture and scoring mechanisms.

E. Pre-contest training (training)

The objectives of CTFs can be gauged from the extent of pre-contest participation it involves prior to the CTF. Some CTFs are purely competitive and all participants compete for winning. There are other CTFs that are far more educational such as Pico, InCTF and MIT/LL CTFs. These have dedicated rounds that enhance learning of specific skills in order to compete in the final round. These learning rounds could also be used to filter participants based on their skill set and performance. This framework allots a higher rating for those CTFs that offer such training sessions.

F. Incentives offered/Awards/ Recognition (incentive)

One of the key driving factors for participation in contests is the incentive the winners receive. The cash or in kind gifts worth certain amount vary between CTFs. Few selected CTFs are so highly recognized in that participation itself is considered for recognition.

G. Total number of participated teams (teams)

The magnitude in terms of number of registered and participating teams reflects the contest size. Larger the participants, the higher are its impact and therefore higher points are given to CTFs that draw large crowds.

H. Assessment of hacking and problem solving skills (improv)

Using surveys that have a combination of questions that are both technical and analytical, the extent of knowledge gain from CTFs can be quantified. To our knowledge this level of correlation is absent. Many times, CTFs being a team event, individual knowledge gain quantification on various aspects of problem solving is also absent. CTFs that include scientific studies are considered superior in their overall design as per this framework.

I. Geographic Reach (locality)

Authorized licensed use limited to: University of Zagreb. Downloaded on October 18,2024 at 15:08:26 UTC from IEEE Xplore. Restrictions apply.
978-1-4799-3759-2/14/$31.00©2014 IEEE

CTF events are compared based on the distribution of participants across the world. Traditionally international contests draw larger participation, hence this framework provide higher points to the same.

J. Scope of the contest (scope)

Restrictions on participation into the contests may depend on various aspects such as age, enrolment in school and/or university or professional career. Some CTFs are open to public and this all-encompassing aspect heavily influences the results. Our recommendation is that participation in a CTF should screen participant background first and then enhance their knowledge.

V. ASSIGNMENT OF WEIGHT TO THE FACTORS USING ANALYTIC HIERARCHY PROCESS

Since all the factors are important, it is difficult to rank them mentally and give weights. Hence Analytic Hierarchy Process (AHP) [20,21] has been used to assign weights. The process makes use of a pair wise comparison matrix. It helps us to compare two factors at a time and put a value from the scale as shown in Table 2.Intensity value indicates the importance of one factor as compared to the others [20].

TABLE III
THE FUNDAMENTAL SCALE OF AABSOLUTE NUMBERS

Intensity	Description
1	Equal importance
2	Equal to moderate importance
3	Moderate importance
4	Moderate to strong importance
5	Strong importance
6	Strong to very strong importance
7	Very strong importance
8	Very to extremely importance
9	Extreme importance

Steps as shown in Table 3 are followed to get weights according to Analytic Hierarchy Process.

TABLE IIIII
STEPS PERFORMED AS PER ANALYTIC HIERARCHY PROCESS

STEP 1	Create a comparison matrix: Ten factors are defined. So a 10 x10 matrix is made listing 10 factors in the row and column, so that comparisons can be made.
STEP 2	Perform comparisons taking two choices at a time. Pick one suitable choice from the scale and assign it to the corresponding part of the matrix as shown in Table 4.
STEP 3	Sum columns of the matrix
STEP 4	Normalize the matrix
STEP 5	Find the average of the rows, this will be the weights for the criteria

TABLE IVV
STEPS PERFORMED AS PER ANALYTIC HIERARCHY PROCESS

	vuln	solv	ratio	period	training	incentive	participants	improv	locality	scope
vuln	1	3	3	7	2	5	8	3	8	9
solv	1/3	1	2	4	3	5	4	3	7	8
ratio	1/3	1/2	1	5	6	4	8	4	5	5
period	1/7	1/4	1/5	1	1/4	2	1/2	2	3	4
training	1/2	1/3	1/6	4	1	5	6	3	6	7
incentive	1/5	1/5	1/4	1/2	1/5	1	4	1/3	4	5
participants	1/8	1/4	1/8	2	1/6	1/4	1	5	8	4
improv	1/3	1/3	1/4	1/2	1/3	3	1/5	1	6	7
locality	1/8	1/7	1/5	1/3	1/6	1/4	1/8	1/6	1	4
scope	1/9	1/8	1/5	1/4	1/7	1/5	1/4	1/7	1/4	1

Consistencies of the weights have been verified. So, Table 5 displays the final framework.

TABLE V
FRAMEWORK WITH FACTORS AND WEIGHTS

Factors	**Weights**
1. Classify the challenges to different categories. Map the categories in to popular software development vulnerabilities and OWASP vulnerabilities (vuln).	25%
2. Check whether tasks are solvable or not (solv)	17%
3. Calculate the ‘difficulty level’ of the task to the ‘solved ratio’ (ratio)	18%
4. How periodic the CTF event is (periodic)	4%
5. Training given prior to CTF (training)	12%
6. Incentives offered/Awards/ Recognition (incentive)	5%
7. Total number of participated teams (teams)	8%
8. Improvement in hacking and patching skills (improv)	7%
9. Locality (locality)	2.5%
10. Scope (scope)	1.5%

Authorized licensed use limited to: University of Zagreb. Downloaded on October 18,2024 at 15:08:26 UTC from IEEE Xplore. Restrictions apply.

VI. ANALYSIS OF THE CTFs PER THE FRAMEWORK

Considering the availability of relevant data, the newly developed framework has been used to rank DEF CON CTF, SECUINSIDE CTF, CSAW CTF, Mozilla CTF and PHD CTF. Table 6 displays the rating process of CTFs.

TABLE VI
RATING OF CTFS

FACTORS	Weights	DEFCON CTF		SECUINSIDE CTF		CSAW CTF		MOZILLA CTF		PHD CTF	
		Points	Final points	Points	Final points	Points	Final points	Points	Final points	Points	Final points
1. Challenge classification and mapping	25%	80.0	20.0	70.0	17.5	50.0	12.5	60.0	15.0	60.0	15.0
2. Solvability of the tasks	17%	80.0	14.0	35.0	6.0	100.0	17.0	100.0	17.0	80.0	14.0
3.Calculate the 'difficulty level' of the task to the 'solved ratio'	18%	80.0	15.0	80.0	14.0	80.0	14.0	60.0	11.0	80.0	15.0
4. Periodicity of the CTFs	4%	100.0	4.0	14.0	0.6	58.0	2.0	5.0	1.0	14.0	1.0
5. Pre-contest training	12%	50.0	6.0	0.0	0.0	50.0	6.0	40.0	5.0	50.0	6.0
6.Incentives offered/Awards/ Recognition	5%	100.0	5.0	75.0	3.8	85.0	4.0	50.0	2.0	50.0	3.0
7.Total number of participated teams	8%	50.0	4.0	95.0	7.6	96.0	8.0	50.0	4.0	25.0	2.0
8.Assessment of hacking and problem solving skills	7%	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
9.Geographic reach	2%	100.0	1.5	100.0	2.5	100.0	1.5	100.0	1.5	100.0	1.5
10. Scope of the contest	3%	100.0	2.5	100.0	1.5	100.0	2.5	100.0	2.5	100.0	2.5
TOTAL POINTS			72.0		53.4		67.5		59.0		60.0

VII. CONCLUSIONS

In the past five years, there has been a steady increase in the number of Capture The Flag (CTF) type of competitions and participation in them by engineering students. Cyber security is a relatively young discipline, automatically attracts the attention of internet generation kids and is linked to technology based competitions like CTF. In the current scenario, there does not exist a frame work to evaluate and rank CTFs. We have created a new framework based on CTF factors like similarity of the tasks to the common critical vulnerabilities, solvability of tasks, periodicity, training given prior to CTF, geographical reach, problem solving skills etc. and assigned weights based on the Analytic Hierarchy Process. Five CTFs have been successfully ranked using the framework and results confirm that factors like Challenge classification, Difficulty level, Solvability of tasks are much more important than factors like pre-contest training, geographical reach, incentives etc.

ACKNOWLEDGMENT

Our work derives direction and ideas from the Chancellor of Amrita University, Sri Mata Amritanandamayi Devi. The authors would like to acknowledge the contributions of faculty and staff at Amrita University whose feedback and guidance was invaluable.

REFERENCES

[1] Sudharsan Sundararajan, Hari N N, Vipin Pavithran, Kaladhar Vorungati, Krishnashree Achuthan, "Preventing Insider Attacks in the Cloud" Advances in Computing and Communications, 2011: p. 488-500

[2] Jayaraj Poroor, Bharat Jayaraman, "DoS Attacks on Real-Time Media through Indirect Contention-in-Hosts," IEEE Internet Computing, vol. 13, no. 6, pp. 22-30, November/December, 2009

[3] Gregory Conti, Thomas Babbitt, and John Nelson, "Hacking Competitions and Their Untapped Potential for Security Education", Vol. 9. Security Privacy, IEEE (2011) 56-59

[4] Kaiyang Zhang, Shihao Dong, "picoCTF 2013-Toaster Wars: When interactive story telling game meets the largest computer security competition", Games Innovation Conference (IGIC), 2013 IEEE International.

[5] Gavas, Efstratios and Memon, N. and Britton, Douglas," Winning Cyber security One Challenge at a Time", Vol. 10. Security Privacy, IEEE (2012) 75-79

[6] Teodor Sommestad, Jonas Hallberg, "Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments", Secure IT Systems Lecture Notes in Computer Science, Volume 7617, 2012, pp 47-60 Springer.

[7] Giovanni Vigna, "The 2010 International Capture the Flag competition", Vol. 9. Security Privacy, IEEE (2011) 56-59

[8] Joseph Werther, Michael Zhivich, Tim Leek, and Nickolai Zeldovich. 2011. Experiences in cyber security education: the MIT Lincoln laboratory capture-the-flag exercise. In Proceedings of the 4th conference on Cyber security experimentation and test (CSET'11). USENIX Association, Berkeley, CA, USA, 12-12.

[9] Ronald S Cheung, Joseph P Cohen, "Challenge based learning in cyber security education" , Proceedings of the 2011 International Conference on Security & Management, Las Vegas, Nevada, USA(2011).

[10] Lexi Pimenidis," Hosting a Hacking Challenge – CTF-style" 2005 RWTH Aachen

[11] Nicholas Childers, Childers, Bryce Boe, Lorenzo Caballero, Ludovico Cavedon, Marco Cova, Manuel Egele, and Giovanni Vigna. 2010. "Organizing large scale hacking competitions". In Proceedings of the 7th international conference on Detection of intrusions and malware, and vulnerability assessment (DIMVA'10), Christian Kreibich and Marko Jahnke (Eds.). Springer-Verlag, Berlin, Heidelberg, 132-152.

[12] http://niccs.us-cert.gov/education/cyber-competition-project-ccp

[13] http://deity.gov.in/content/national-cyber-security-policy-2013-1

[14] Dino Schweitzer, David Gibson, David Bibighaus, Jeff Boleng, "Preparing Our Undergraduates to Enter a Cyber World", Information Assurance and Security Education and Training IFIP Advances in Information and Communication Technology Volume 406, 2013 Springer, pp 123-130.

[15] Joshi, A. and Ramani, V. and Murali, H. and Krishnan, R. and Mithra, Z. and Pavithran, V., "Student centric design for cyber security knowledge empowerment", Technology Enhanced Education (ICTEE), 2012 IEEE International Conference on, Pages1-4.

[16] Mike O'Leary , "Small-Scale Cyber Security Competitions" , Proceedings of the 16th Colloquium for Information Systems Security Education ,Orlando, FL June 11-13, 2012

[17] Collins, M., Schweitzer, D., and Massey, D., "CANVAS: a regional assessment exercise for teaching security concepts," in Proceedings from the 12th Colloquium for Information Systems Security Education, June 2008.

[18] LCDR Chris Eagle, and John L. Clark," Capture-The-Flag: Learning Computer Security Under Fire", Naval Postgraduate School , JUL 2004

[19] Sebastian Koch, Joerg Schneider and Jan Nordholz," Distributed playing: Another kind of educational security game", In Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test (CSET'12). USENIX Association, Berkeley, CA, USA, 11-11.

[20] Thomas L Saaty,"How to make a decision: The analytic hierarchy process", European Journal of Operations Research, Volume 48, Issue 1, 5 September 1990, Pages 9–26

[21] Thomas L Saaty, Luis G Vargas ,"How to make a decision", Models, Methods, Concepts & Applications of the Analytic Hierarchy Process International Series in Operations Research & Management Science Volume 175, 2012, pp 1-2

Authorized licensed use limited to: University of Zagreb. Downloaded on October 18,2024 at 15:08:26 UTC from IEEE Xplore. Restrictions apply.