Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2018) 26: 1977 – 1988

doi:10.3906/elk-1710-266

Presenting a method to perform cyber maneuvers

Mohammad SHAKIBAZAD[1,*], **AliJabar RASHIDI**[2]

[1]Department of Information and Communications Technology, Malek-Ashtar University of Technology, Tehran, Iran
[2]Department of Electrical Engineering, Malek-Ashtar University of Technology, Tehran, Iran

Received: 02.11.2017 • **Accepted/Published Online:** 08.04.2018 • **Final Version:** 27.07.2018

Abstract: Performing cyber maneuvers in an operational environment is not easy. We need a cyber-situational awareness framework to perform its maneuvers to protect the cyberspace and to cope with its attacks. The battlefield provided has essential information for detecting cybercrime events. The present study resolved the challenges of implementing these maneuvers through dynamic simulation of the cyber battlefield. The cyber battlefield contains detailed information on cyberspace elements, including the vulnerability knowledge repository, the tangible and intangible components of the cyberspace allowing maneuvering, penetration testing, injection attacks, tracking attacks, visualization, evaluation of the impact of cyberattacks, and risk evaluation. By injecting attacks and using the proposed algorithms, an impact assessment of each attack step on each of the elements of the environment has been done to identify potential threats. Using the proposed algorithms, an impact assessment has been performed on each of the environmental elements in order to identify potential threats. A dynamic updating simulator engine has been designed to update the vulnerability knowledge base automatically and change the topology and features of elements, accesses, services, hosts, and users. Modeling and simulation were evaluated using a qualitative research method and creating a focus group.

Key words: Cyber maneuvers, cyber defense, cyberspace simulator, cyber battlefield

1. Introduction

The complexity of defense against attacks has increased and so has the complexity of cyberspace. Cyberattacks can have unpleasant consequences in military networks as well as in civilian infrastructure [1]. The nature of wars has changed from military to cyber. In these attacks, the major infrastructure of the country is attacked remotely through cyberspace. What an attacker gains by breaching the cyberspace of others is far more valuable than land occupation. The risk of cyberattacks is not less than that of military action, with lethal consequences for governments. Hence, special attention to this area is essential. The production of indigenous knowledge in this area is of utmost significance. The most valuable asset of any organization to be protected is information, especially financial and banking information. In upstream documents in the cyber security of countries, the existence of an indigenous model of cyber security has been stressed, as cyber security is an important part of national security.

One of the issues is vulnerabilities' identification in cyberspace assets. Organizations are heavily dependent on IT infrastructure and cyberspace; therefore, breach, sabotage, and disclosure of information of the organizations will have high costs. Thus, ensuring the secured nature of this environment is essential. Another issue in the identification of network vulnerabilities is the software and hardware existing in cyberspace. Given

*Correspondence: shakibazad@gmail.com

the implementation problems of penetration tests, such as being costly, the possibility of service interruption, and lack of complete trust in the companies running the penetration test, provision of a solution for implementing cyber maneuvers out of the real and physical environment in organizations is necessary. For cyber defense, a situational awareness system is needed to provide the analyst with complete and accurate information about the status of cyber components. The purpose of this study is to provide cyber defense tools based on situational awareness to make timely and correct decisions to deal with cyberattacks. As no comprehensive models have been presented for this area, an indigenous model needs to be devised in this regard.

2. Basic notions

This section deals with the basic concepts of the study, including cyber situational awareness (CSA), vulnerabilities, the model, cyberspace, and, finally, the literature.

Situational awareness is the awareness of what is happening in cyberspace and its surroundings, as a cognitive process able to figure out the status quo of cyberspace and decide based on its meaning. Situational awareness consists of three levels: 1) perception of elements in the current situation, 2) comprehension of the current situation, 3) projection of the future status of reception [2].

According to the definition of the European Union Agency for Network and Information Security, vulnerability is the existence of weakness or error in design or implementation error that can lead to sudden and unpleasant events compromising security and violating security policies of the system, network, software, or protocol. Breaching happens through exploiting vulnerabilities [3]. Thus, one of the basic factors in modeling and simulation is the cyber battlefield.

A model or pattern is a simplified sample of reality. Patterns and models may have mental imagery, graphic displays, expressions, or mathematical representations of reality. Hence, patterns and models imply implicit references to the static image of reality [4].

Every environment, including cybernetic ones, contains components and elements. The elements of a cyber battlefield are tangible and intangible components along with the communication between them [5].

3. Related work

An attack graph determines the possibility of breaching from a given start point to a computer network. The work in [6] used an attack graph to evaluate vulnerabilities, while [7] conducted a comprehensive review of the attack graphs. Attack graphs are acyclic graphs that show different possible steps for an attack. In most implementations, each graph can model only one goal. According to [7], one of the problems is the implementation of the attack graph model. As these graphs are not cyclic, in an attack graph, the relations between hosts cannot be modeled. Thus, it is necessary to create multiple graphs for modeling these communications, and multiple attack graphs have to be created for multiple purposes. As a cyber battlefield has no boundary restrictions, it will not have the problem of attack graphs, i.e. all transfers can be modeled in just one battlefield. Among the other reasons is assuming a static relationship between nodes. Given the firewall and routers, it is impossible to assume that different traffic is created between 2 authorized or unauthorized hosts. The challenge is covered in the proposed model, as well. In the cyber battlefield model, firewall rules and access lists are considered. Thus, the information needed to detect the permissibility of the traffic exists.

A vulnerability tree is an attack graph modeled like a tree. The root of the tree is the ultimate goal of the attack; the leaves show the logical starting points and the nodes of other stages of the attack. Scrolling from a leaf to the root shows a possible sequence of attacks. Each node has a structure showing the complexity of the

attack. With the help of vulnerability trees, [8] tried to evaluate vulnerability and [9] used vulnerability trees to enhance security. Vulnerability trees, like attack graphs, face the challenge of scalability. As a vulnerability tree is defined to attain an objective, the trees need to be defined for multiple targets and multiple vulnerabilities. This method of definition makes the vulnerability tree very difficult for a large network because we need to define large and complex vulnerability trees. This problem is resolved in the proposed model of a cyber battlefield and is implicitly capable of modeling all known attacks and targets in a single model. The scalability of the cyber battlefield depends only on the scalability of the algorithms used in analysis of the cyber battlefield. In the vulnerability tree, like the attack graph, communications between hosts are assumed static with no firewall rules. Defining a new attack or changing network configuration can dramatically change the structure of the vulnerability tree. As the network changes or the type of attack or firewall rules lead to small changes in the cyber battlefield model, the attacking stages by the cyber battlefield are not modeled explicitly.

The work of [10] explained and compared the impact and threat prediction with the help of sampling. In this study, the impact assessment was designed to estimate the damage caused by the attack, with sensitivity coefficients not considered. The work of [11] developed a framework for modeling cyberattacks using attack graphs and impact assessment. In this study, prototyping was used to describe and evaluate the model's performance. They used real-time event analysis methods for predicting future stages of the attacks and evaluating the impact of attacks to analyze and build an attack graph. The main weakness of this study was related to the scalability problems of attack graphs. The work of [12] presented a model for the computer network to evaluate the network's defense mechanisms with moving goals. The purpose of this modeling was to change the network properties to mislead the attacker. They used dynamic IP address change, dynamic port, and firewall change in the cyberattack simulator. In [13], multistage network attacks were simulated by fusion of the conceptual model. The simulator, called MASS, dealt with network modeling, hierarchical vulnerability structure, and attack behavior and attack scenario. In [14] the authors investigated the impact of cyberattacks on a computer network. They also mentioned previous studies on this issue. Furthermore, [15] presented a simulation of cyberattacks with a distribution approach. Distribution enables people and programs to interact in different geographic locations. This simulator is available in 2 analytical and interactive modes, which are used to identify some weaknesses in the network.

Threat intelligence (TI) means evidence-based knowledge representing threats that can inform decisions. There is a general awareness for the need of threat intelligence, while vendors today are rushing to provide a diverse array of TI products, specifically focusing on technical TI. Although TI is being increasingly adopted, there is little consensus on what it actually is or how to use it. Without any real understanding of this need, organizations risk investing large amounts of time and money without solving existing security problems [16–18]. Our paper is new approach to cyber threat intelligence to help protect organizations. The aim is to use this framework to gather TI that will improve the efficiency and effectiveness of risk management, automate their processes, and allow them to go search for potential threats and stop them before they happen.

The work of [19] introduced 2 concepts for risk assessment methods: first, an interdependency relationship among the risk scores of a network ?ow and its source and destination hosts, and second, a concept that they called ?ow provenance, which represents risk propagation among network ?ows considering the likelihood that a particular ?ow is caused by the other ?ows. Based on these 2 concepts, they developed an iterative algorithm for computing the risk score of hosts and network ?ows. The work of [20] explored the permission-induced risk in Android apps on three levels in a systematic manner.

One of the tools presented in the field of cyber security is the security operation center. This tool identifies

potential attacks by collecting, correlating, and fusing alerts from security sensors. This tool is effective only during or after the attack, and since there is no possibility of attack injection and simulation in these tools, it cannot be used for preventive, safety, or maneuvering measures. In a part of their review paper, by posing the challenges and limitations of the impossibility of validating and verifying, the authors of [21] indicated that the field was new and immature.

The novelty of the paper is providing a model of an integrated cyber battlefield, including the service model, vulnerability, host, network, and algorithms (risk evaluation, impact scores, sensitivity coefficients, logical attack) for attack injection and security analysis. The dynamic updating engine has a real-time role in the dynamic development of the battlefield. The graphical representation of the analyses consists of graphs for impact assessment of attack and tracking the attack on a network topology. When vulnerability is detected and recorded, it takes some time to inform the security media. Many breaches occurring during this time are resolved in this study. Malware has become a big threat to information systems, which are widely used to store, transfer, and process information for many critical assets [22]. The work in [23] proposed an improved framework for more secure authentication and authorization. Malicious software exploits vulnerabilities, most of which are publicly available. As a result, identifying and managing vulnerabilities is essential [23,24].

One of the issues of the information security field is the lack of tools to provide security solutions to improve the overall security of the network. As buying security equipment and network equipment, purchasing or upgrading software, and changing network configuration have high costs, the battle with security analyses it performs by injection of various types of attacks offers some prioritization and suggestions to network administrators to improve the network security level. Concerning the studies in this regard, there are just a few related papers. Studies and activities in the field of military and cyber security have been categorized. One of the limitations is the lack of databases and related papers for confidential reasons. As shown in the theoretical foundations, prototyping has been used in several papers, such as [10,11], to compare and evaluate the model's performance. Thus, the present paper has used prototyping and simulation. In a previous article [5], general concepts of cyber situation awareness and an example of a vulnerability tree were explained. In this paper, the cyberspace simulator and its results are explained.

4. Method

Object-oriented methods provide the ability to model real-world phenomena. We show cyberspace as a set of objects, attributes, behaviors, processes, communications, and data interactions. Object-oriented methods are inspired for modeling physical, nonphysical, communication, and process components. Therefore, the design is implemented in a way that is flexible against information and behavioral changes. This method is also used in the simulator implementation.

5. Model assessment method

When focusing on qualitative/detailed data about people's views of phenomena, the focus group approach can be used. Researchers using a descriptive survey method can use this method to interpret quantitative data after collecting it. In order to evaluate, verify, and prove the accuracy of the modeling and its accuracy, we used the qualitative research method of the focus group. First, modeling is evaluated in the focus group; then, by simulation, the model's accuracy in the focus group will be analyzed and evaluated [25].

Given that the purpose is security analysis of the network of large organizations, real sampling is performed in large and relatively large networks with a relatively high level of security and diverse services.

Nevertheless, experts need to be selected from a community that has enough expertise in the field of information security and a multiyear career background. The network of the selected sample for the battlefield simulator was implemented and the simulator results were compared to the actual results from the security equipment. The focus group was formed of 6 cyber security and network security experts with a minimum of 5 years of senior management experience from among the technical staff. The acceptable error rate for algorithms was considered to be at most 15% and, by this criterion, algorithms were optimized to reach the desired result. In each session, the results were reviewed and compared, and with the participation of all groups, the deviations were identified. After corrections were made to review the results, the next meeting was held. Four meetings were held within a month to agree on the results.

According to the feedback from the focus group, the necessary modifications were made to the modeling simulation sections and reviewed during the following sessions. After some sessions and with some modifications, the focus group confirmed all the raised issues.

6. Results and discussion

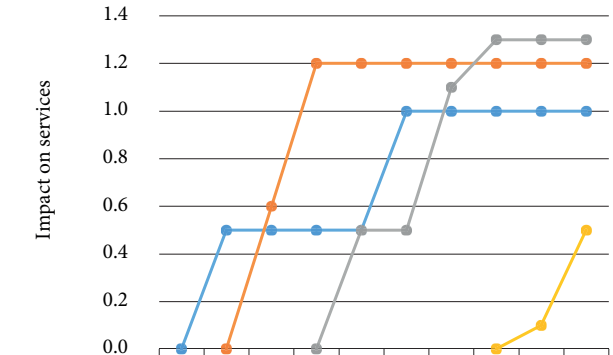
6.1. Flowchart of performing cyber maneuvers

The flowchart of performing cyber maneuvers is shown in Figure 1. To obtain the CSA, we first have to understand the current state of the environment, and we need to identify the characteristics of the components of the environment and then the vulnerabilities of each of the components. The steps and sequence of the process are shown in Figure 1, as follows. Step 1: Extraction, standardization, and storage of all public vulnerabilities from references, topology, and specification of network components and network image production. Identify the vulnerabilities of each service and map between services and vulnerabilities and create a vulnerability tree and a service tree. Step 2: Collecting the necessary information, creating a scenario of attacks (using 2 methods, online or using the attack simulator), storing scenarios of attacks on the battlefield. Step 3: Create a knowledge base of the integrated battlefield model and dynamic update. Step 4: Attack injection, risk assessment, impact assessment, and graphic representation of the attack path on the battlefield; graphically display the results of the algorithms (visualization).

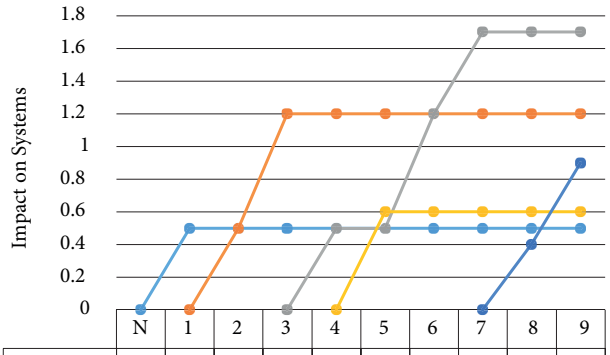
If we want to perform cyber maneuvers in a nonoperational environment, the attack alerts (or directly attack scenarios) are generated by the attack simulator and injected into the battlefield, and then the impact and risk are evaluated. In this situation, it is possible to inject different types of attacks with different characteristics into the battlefield automatically and by analysis of the results one can identify the weaknesses and vulnerabilities in the cyberspace. Helped by these analyses, the battlefield manager can take steps to secure the network elements and network topology in the simulator environment by changing the network topology, network configuration, access list, hardware, and software upgrades, adding and moving security sensors. After implementation of the new configuration in the next step, the network administrator evaluates the battlefield's resistance by more extensive attack injection. In this situation, one can predict which security configuration can provide the highest level of resistance for the cyber environment. Subsequently, subsystems of the cyber battlefield are introduced.

6.2. Creating a network image and vulnerability knowledge base

The network environment includes tangible and intangible components along with communication between them. Tangible components are the ones such as workstations, servers, firewalls, routers, users, detection systems, and breach prevention systems. Network scanners and configuration files collect this information



	N	1	2	3	4	5	6	7	8	9
web	0.0	0.5	0.5	0.5	0.5	1	1	1	1	1
webmail		0	0.6	1.2	1.2	1.2	1.2	1.2	1.2	1.2
telnet				0	0.5	0.5	1.1	1.3	1.3	1.3
realplayer								0	0.1	0.5



	N	1	2	3	4	5	6	7	8	9
e web	0	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
mail		0	0.5	1.2	1.2	1.2	1.2	1.2	1.2	1.2
d4 w				0	0.5	0.5	1.2	1.7	1.7	1.7
i web					0	0.6	0.6	0.6	0.6	0.6
d3 w								0	0.4	0.9

Attack Step	1	2	3	4	5	6	7	8	9
Impact on Network	1	1	2	2	3	4	4	4	5

Figure 1. Flowchart of performing cyber maneuvers.

from the network environment. The service, host cluster, protocol, vulnerability, and attack scenario are the intangible components. The component of battlefield communication is also the list of access between the components and rules of the firewall. Preprocessing and integrating this information is done by this subsystem, and in the next step, according to these standards, normalization of information is done and finally the network administrator can monitor and complete the topology of the network.

The vulnerabilities discovered in daily cyberspace are recorded in some basic references. Besides these references, some standards have been developed to classify and scan vulnerabilities, and this information in needed to understand the current state of the cyberspace. By integration, correlation, and categorizing of vulnerabilities, the vulnerability knowledge base generator creates and updates the process. Each server or workstation in cyberspace contains several active services that can contain vulnerabilities. Identification of the vulnerability of services and other components of the battlefield is done by the dynamic battlefield engine. Solving the problem of automatic identification and the moment of the vulnerability and its announcement in cyberspace are done in this section. In the first step, all vulnerabilities registered from vulnerability registry sources are collected and stored in the knowledge base by performing necessary processes and communicating between services. Then an agent and an automated and online robot are checked on the Internet at short intervals and updated if necessary. If a new vulnerability is detected and in the battlefield intended underlying services of the impact of this vulnerability are used, the network administrator will be given the necessary alerts and information to quickly resolve the problem or interrupt the service until the problem is resolved.

6.3. Situational awareness knowledge base

The knowledge of the components of the battlefield for the use of the algorithms needs fusion, preprocessing, normalization, and integration, and ultimately it needs to be saved in the knowledge repository. Moreover, every subsystem in the situational awareness system produces knowledge. These data are also converted into a standard database by the cyber battlefield generator and kept in the knowledge repository.

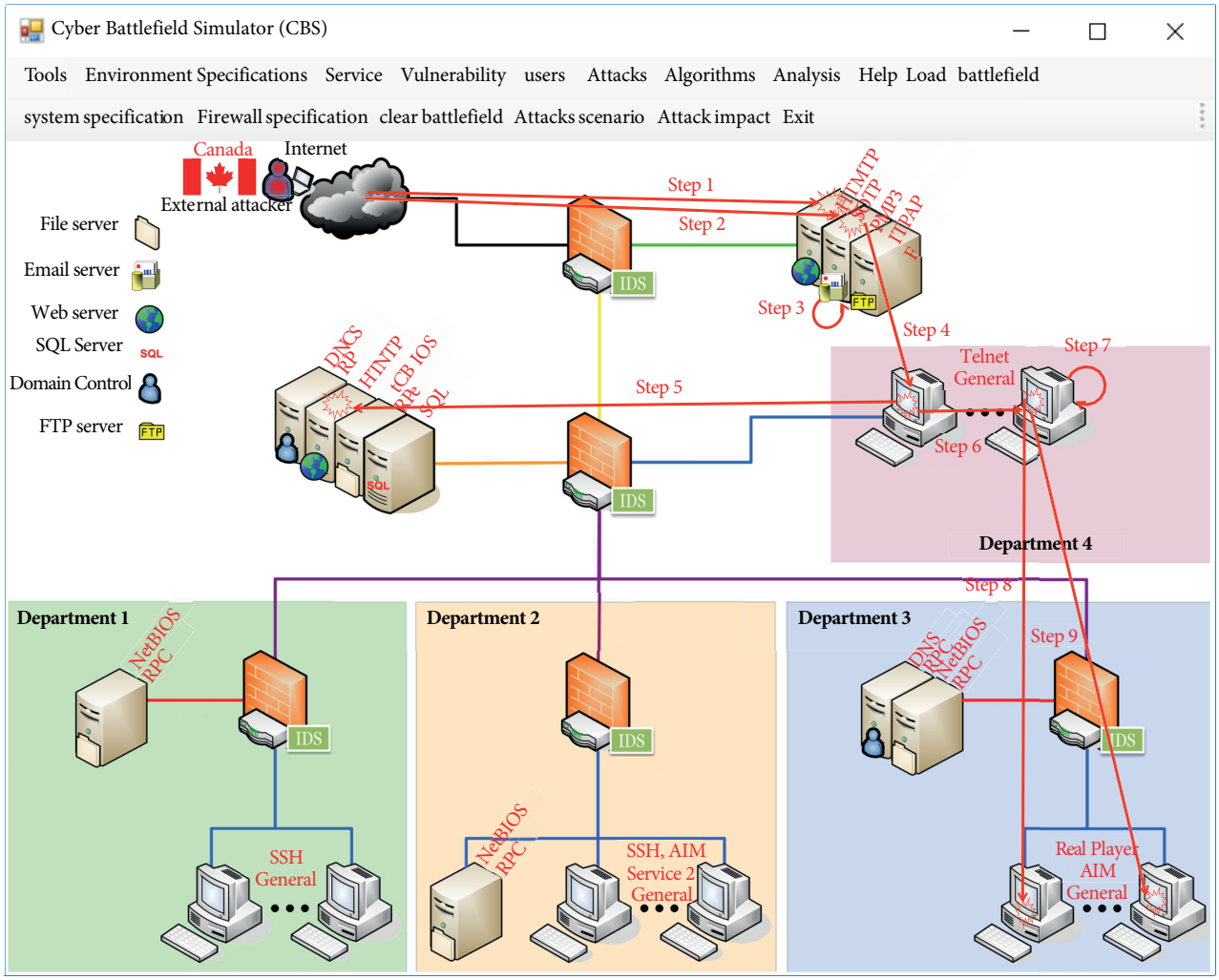


Figure 2. Cyber battlefield simulator (CBS).

6.4. Cyber battlefield tree structure

The main inputs of the model include sensor-correlated alarms, environment component information (host, service, router, firewall, and users), and vulnerability information. The cyber battlefield engine generates a cyber battlefield model in a tree structure by integration and fusion of the network model, vulnerability model, service model, and attack path. It is possible to observe the components used in the battlefield as well as their features in this structure. Each node, like the workstation, has features related to cyberattack scenarios such as IP address, access list, active services, breach detection/prevention system, Internet accessibility, time-based status, status quo, operating system, and sensitivity factor.

6.5. Simulation algorithms

The cyber battlefield is a good ground to conduct security analyses. The analytic algorithms used are described below.

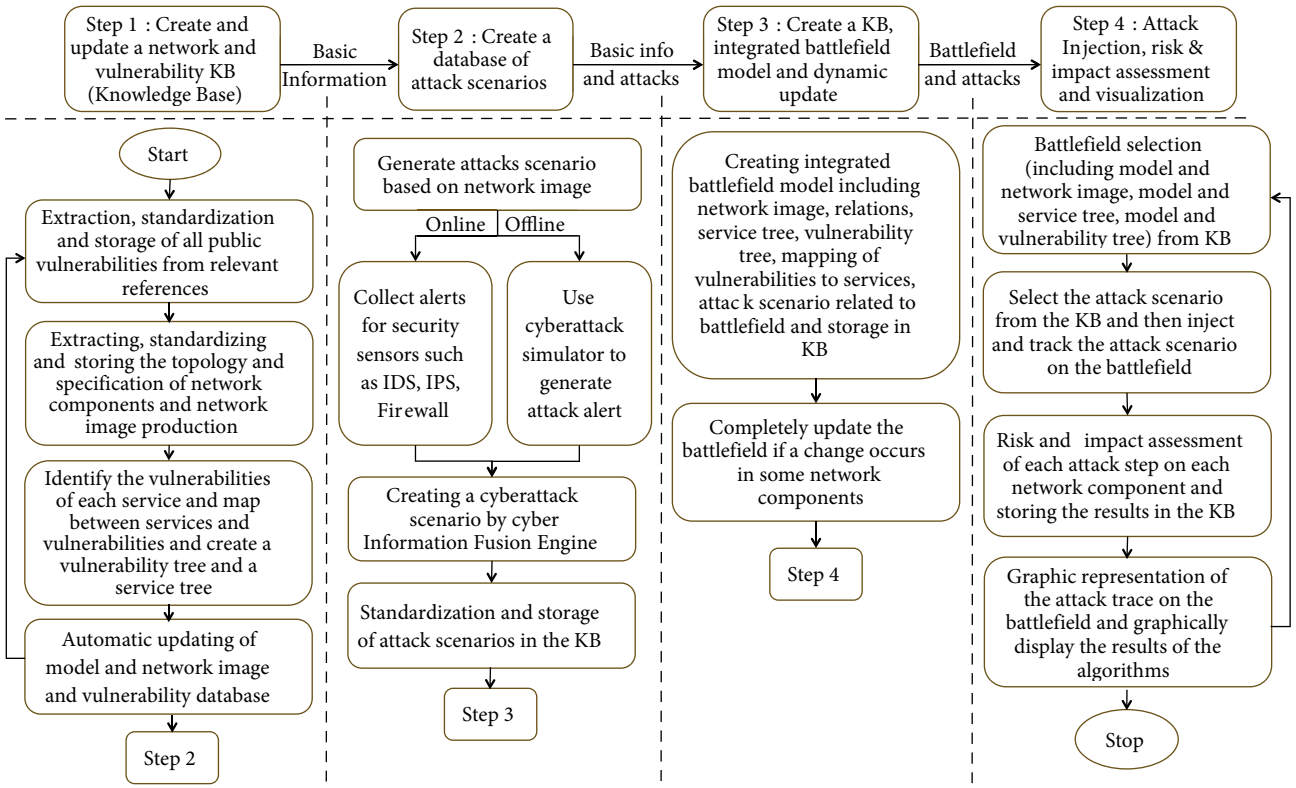


Figure 3. Charts related to the results of the impact assessment algorithms.

6.6. Calculation of sensitivity coefficients

The sensitivity coefficient is used to determine the sensitivity of an element in a cyberspace used in risk and impact evaluation. The network administrator and the focus group generate the sensitivity coefficient for the range, mission, and type of attack step. The common vulnerability scoring system framework calculates the sensitivity coefficient. For each service, at least one mission is determined, each of which has a different degree of importance. For example, the importance of the database service mission is higher than the file sharing service mission. The value of the coefficients of sensitivity is between 0 and 1, with zero sensitivity showing the nonrelevance of that component to the mission and sensitivity of 1 showing the full necessity of that component for the fulfillment of the mission.

6.7. Risk assessment

The purpose of risk management is to protect the organization for its mission, which can be divided into 2 main domains: risk assessment and reduction areas. Risk assessment of a service across the entire network is the sum of the sensitivity of the vulnerability scores of the service divided by the number of vulnerabilities in 10. According to the relationship, the higher the number of vulnerabilities and the sensitivity of vulnerabilities coefficients, the higher is the risk of that service and vice versa.

6.8. Impact assessment of the attack on the battlefield components

The impact assessment is done to determine the extent to which the attacker's attack on each of the network components is destructive. For injection of each step of the attack to the battlefield, the impact evaluation is performed on each component of the battlefield (service, host, user, and the entire network). Evaluation of the total network impact is calculated based on the value of final damage to the entire network components.

6.8.1. Impact on services

The impact on service is the damage to a service due to an attack step. The effect of the step of the attack m on the service n (Eq. (1)) is equal to the sensitivity of the attack type multiplied by the service sensitivity n multiplied by the maximum sensitivity rating of the used vulnerabilities (k set) at the step of the attack m at time t.

$$\mathrm{I}mpactServic_n\left(AttackStep_m\right) = Sensitivity\left(\mathrm{AttackStep}\right) * Sensitivity(Servic_n) * (cvss(vul_k)); [0.1] \quad (1)$$

6.8.2. Impact on hosts

The impact on the host is the damage to a host due to an attack step. The effect of step m on the host n (Eq. (2)) is equal to the host sensitivity coefficient n multiplied by the maximum effect obtained from attack m step on the host services n (k set) at time t.

$$ImpactHost_n\left(AttackStep_m\right) = Sensitivity\left(Host_n\right) * \left(ImpactService_k\right); [0.1] \quad (2)$$

6.8.3. Impact on users

Each user uses different hosts. The user's effect is the damage each user suffers because of an attack, resulting in a number of users being affected by each step of the attack. The effect of attack step m on user n (Eq. (3)) is equal to the user's sensitivity coefficient n multiplied by the maximum host effect obtained from m attack step on the user hosts n (k set) at time t.

$$ImpactUser_n\left(AttackStep_m\right) = Sensitivity\left(User_n\right) * \left(ImpactHost_k\right); [0.1] \quad (3)$$

6.8.4. Impact on the total network

The total network effect is the damage to the entire network due to the implementation of an attack step. The effect of attack step m on the entire network is equal to the sum of the impact of the victim's hosts until step m attack. Given that this score is obtained from the integration of the host score (also the rating of services and network vulnerabilities), it enables the network to be monitored by security analysts and network administrators.

6.8.5. Scores of reference impact

For having a base for comparing and calculating the damage, we need the reference points for each effect score. The reference point is the highest point of the item that that component can have. For instance, a host's reference rating means exploiting all vulnerabilities in its hosting services with the highest damage rating. A user rating point shows the highest possible effect of the hacking of all hosts on that user.

Table. Attack scenario specifications.

Step	Source IP	Dest IP	Port/Prot	Description	Alert Signature	CVE ID
1	149.56.155.123	192.168.1.2	80/tcp	Recon Enum	WEB-MISC http directory traversal	CVE-2007-1860
2	149.56.155.123	192.168.1.3	143/tcp	Intrusion Root	IMAP authenticate overflow attempt	CVE-2005-2278
3	192.168.1.3	192.168.1.3	143/tcp	Intrusion Root	IMAP authenticate overflow attempt	CVE-2005-2278
4	192.168.1.3	192.168.4.100	23/tcp	Intrusion User	TELNET EZsetup account attempt	CVE-2001-0347
5	192.168.4.100	192.168.3.3	80/tcp	Recon Enum	WEB-MISC http directory traversal	CVE-2007-1860
6	192.168.4.100	192.168.4.104	23/tcp	Intrusion Root	WEB-MISC telnet attempt	CVE-2004-0568
7	192.168.4.104	192.168.4.104	ICMP	Recon Scanning	ICMP Traceroute	PING
8	192.168.4.104	192.168.31.100	ICMP	Recon Scanning	ICMP Traceroute	PING
9	192.168.4.104	192.168.31.103	276/tcp	Goal Dos	DOS Real Audio Server	CVE-2002-0337

6.9. Attack injection

The implementation of the subsystems and modules provided in the architecture (Figure 1) is implemented in the cyber battlefield simulator (Figure 2). The sample attack scenario for injection to the simulation has 9 steps aimed at attacking the web server, mail server, telnet server, and RealPlayer (Table). After attack injection to the battlefield, the results of its tracing are presented in Figure 2 and the results of the impact assessment in Figure 3. According to the battlefield database, the attack originates in Ontario (Canada) and the largest damage was introduced to Departmental Workstation 1, Department Administrator 1, and the internal Web server. The grid effect of the network indicates the effect of the attack on the entire network. It is assumed that the steps of the attack are implemented successively and without interruption. As already stated, one of the issues is the lack of a tool to provide security solutions with the ability to prioritize to enhance the security of the entire network. Selecting optimized security architecture, preferably with the fewest changes and minimum cost, which can get a satisfactory level of security, is a problem for network administrators provided for on the proposed battlefield. For instance, after the analysis in the sample network, it was shown that the greatest breaches were due to the misuse of Windows FTP service vulnerabilities, which will greatly enhance the level of network security by upgrading the service and its operating system.

6.10. Conclusions and suggestions

One of the most important components of cyber command and control is cybercrime awareness. We need accurate monitoring and cyber maneuvers to obtain cognitive status awareness. The battlefield engine provides the necessary information for security analyses by creating a situational knowledge repository including the updated security vulnerabilities, attack scenarios, service model, network model, and cyber battlefield model. Dynamic updating, tracking, matching attacks, statistical analyses, and information relations of situational awareness are among the tasks of the battlefield engine. The algorithms presented in the subcategory of risk and vulnerability evaluation detect and evaluate the potential threats of the cyberspace, and by cyberattack injection, tracking and attack effect analysis of the network are performed. Graphical representations of topology, network component status, attack track, statistical analyses, user relations management, effect, and risk assessments are done by the visualization subsystem. As seen in the results section, cyber maneuvers, network threats, and network vulnerabilities can be implemented with this simulator. Focus groups are selected as a qualitative research methodology to evaluate modeling. This model can be generalized for all projects and organizations. The ultimate goal is to provide a cyber defense tool based on situational awareness to provide proper and timely decision making to deal with cyberattacks. Implementation of the battlefield simulation using agent-based modeling is proposed for future studies. In this method, battlefield components such as hosts, attackers, firewalls, security sensors, and services are considered as the elements.

References

[1] US Air Force. United States Air Force Cyberspace Science and Technology Vision 2012-2025. Washington, DC, USA: US Air Force, 2012.

[2] Endsley MR. Toward a theory of situation awareness in dynamic systems. Hum Factors 1995; 37: 32-64.

[3] Meshkini A, Habibi K, Alizadeh H. Using fuzzy logic and GIS tools for seismic vulnerability of old fabric in Iranian cities (case study: Zanjan city). J Intell Fuzzy Syst 2013; 25: 965-975.

[4] Lotfian S. Strategy and Strategic Planning. Tehran, Iran: Ministry of Foreign Affairs, Political Science, 1997 (in Persian).

[5] Shakibazad M, Rashidi AJ. A framework to achieve dynamic model of cyber battlefield. Soc Roy Sci Liège. 2017; 86: 474-483.

[6] Phillips C, Swiler LP. A graph-based system for network-vulnerability analysis. In: Proceedings of the 1998 Workshop on New Security Paradigms; 1998; New York, NY, USA. pp. 71-79.

[7] Lippmann RP, Ingols KW. An Annotated Review of Past Papers on Attack Graphs. Cambridge, MA, USA: MIT Lincoln Laboratory, 2005.

[8] Vidalis S, Jones A. Using Vulnerability Trees for Decision Making in Threat Assessment. Pontypridd, UK: University of Glamorgan School of Computing, 2003.

[9] Schneier B. Attack trees. Dr Dobbs J 1999; 24: 21-29.

[10] Yang SJ, Holsopple J, Liu D. Elements of impact assessment: a case study with cyber attacks. In: Intelligent Sensing, Situation Management, Impact Assessment, and Cyber-Sensing; 2009; New York, NY, USA. p. 8.

[11] Kotenko I, Chechulin A. A cyber attack modeling and impact assessment framework. In: 5th International Conference on Cyber Conflict; April 2013; Tallinn, Estonia. pp. 1-24.

[12] Wheeler BF. A Computer Network Model for the Evaluation of Moving Target Network Defense Mechanisms. Rochester, NY, USA: Rochester Institute of Technology; 2014.

[13] Moskal S, Wheeler B, Kreider D, Kuhl ME, Yang SJ. Context model fusion for multistage network attack simulation. In: IEEE Military Communications Conference; 2014; New York, USA. pp. 158-163.

[14] Kott A, Wang C, Erbacher RF. Cyber Defense and Situational Awareness. New York, NY, USA: Springer, 2015.

[15] Ashtiani M, Abdollahi Azgomi M. A distributed simulation framework for modeling cyber attacks and the evaluation of security measures. Simulation 2014; 90: 1071-1102.

[16] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur 2018; 72: 212-233.

[17] Qamar S, Anwar Z, Rahman MA, Al-Shaer E, Chu BT. Data-driven analytics for cyber-threat intelligence and information sharing. Comput Secur 2017; 67: 35-58.

[18] Mavroeidis V, Bromander S. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: European Intelligence and Security Informatics Conference; 11–13 September 2017; Karlskrona, Sweden. pp. 91-98.

[19] Rezvani M, Sekulic V, Ignjatovic A, Bertino E, Jha S. Interdependent security risk analysis of hosts and flows. IEEE T Inf Foren Sec 2015; 10: 2325-2339.

[20] Wang W, Wang X, Feng D, Liu J, Han Z, Zhang X. Exploring permission-induced risk in Android applications for malicious application detection. IEEE T Inf Foren Sec 2014; 9: 1869-1882.

[21] Nguyen PH, Ali S, Yue T. Model-based security engineering for cyber-physical systems: a systematic mapping study. Inform Software Tech 2017; 83: 116-135.

[22] Bayoğlu B, Soğukpınar İ. Polymorphic worm detection using strong token-pair signatures. Turk J Electr Eng Co 2009; 17: 163-182.

[23] Jiang W, Xu H, Dong H, Jin H, Liao X. An improved security framework for Web service-based resources. Turk J Electr Eng Co 2016; 24: 774-792.

[24] Uğur A, Soğukpınar İ. Multilayer authorization model and analysis of authorization methods. Turk J Electr Eng Co 2016; 24: 4915-4934.

[25] Bazargan A. An Introduction to the Qualitative and Mixed Methods Research Approaches Used in Behavioral Science. Tehran, Iran: Didar, 2010 (in Persian).