Attack Tree Visualization for Cyber Security Situational Awareness

M. Selvi, E. B. Aksu, M. H. Dilek, A. Erkan, and M. U. Demirezen

***Abstract*— Situational awareness in cyber domain is one of the key features for quick and accurate decision making and anomaly detection. In order to provide situational awareness, certain methods have been introduced so far and attack graph is one of them. Attack graphs help the security analyst to visualize the network topology and understand typical vulnerability and exploit behaviors in cyber domain (e.g., IT asset and the network). They provide more proactive view compared to other reactive views; hence risk management and evaluation can be done in an efficient and interactive fashion. Attack trees can be used for various purposes since they can map network assets, network attacks and possible vulnerabilities which may exist in the IT assets. This study introduces an integrated cyber security capability called, BSGS, which can help analysts to create attack trees, identify vulnerabilities and have effective risk assessment procedures. In this way, the cyber security specialists will have a more efficient and holistic way to assess their environments and take the most effective precautions to minimize cyber risks.**

***Index Terms*—attack graph, attack tree, cyber security, risk assessment, situational awareness**

I. Introduction

THROUGHOUT the 2000s, the term, cyber security, has become a household term. Cyber attacks became more frequent than ever. Serious and coordinated attacks had been experienced all over the world and the damages were quite non-ignorable. Thus, for the last ten years the nation states started to invest more in developing their own security and defense systems and make their preparations to fight with cyber threat. So, a new era was born as a fifth to modern warfare and the term, cyber security and defense, began to be heard more in nation states and military organizations such as NATO [1].

Cyber security can be defined as the information security for protection of cyber space and assets including tools, policies, security safeguards, guidelines, risk management approaches, assurance and technologies, etc... [2] In this cyber space, including users, networks and devices, the main objective is to secure and store data safely by means of comprising CIA (Confidentiality, Integrity and Availability) and enable uninterrupted and secure operation of business [2].

M. Selvi, E. B. Aksu, M. H. Dilek, A. Erkan, and M. U. Demirezen, STM Cyber Security Group

With increasing needs in cyber security platform, quick and accurate decision making become more and more important for being aware of the attacks and reacting as fast as possible [3]. For this reason, cyber situational awareness started to play a critical role and the need for systems having such capabilities has increased. Situational awareness provides the processes identifying both domain specific and cross domain activities [3]. These processes can be related to the system environment, the domains, the aims and the decisions of the users.

In order to provide situational awareness, attack visualization is a must to help decision makers to understand the baseline behaviors and detect anomalies in a network [4]. Several visualization methods have been introduced since the situational awareness against cyber attacks started to be a must-have capability. Among them, the most popular one is attack graphs. By using them, security specialists can detect critical security bottlenecks and identify vulnerabilities which are at the heart of particular system [5].

There are many ways to represent attacks. One of them is using attack trees. It is the best known way to categorize the attacks with different nature which target the defended networks [6]. Firstly introduced by Schneier [7], [8], it has become the most trustworthy and consistent way to detect vulnerabilities proactively [l]. This graphically structured tree notation is also selected as an easy and understandable way for implementing attack vector.

In this study, brief information about the terms - situation awareness, attack graphs and attack trees - will be given and Integrated Cyber Security System (Turkish: Bütünleşik Siber Güvenlik Sistemi, "BSGS") will be introduced as the answer to these needs. This system uses attack trees in order to evaluate risks based on vulnerabilities and calculate multi-step attacks. By using vulnerabilities and risks, the system maps the paths of attacks and gained privileges of attackers. The system provides an interactive method which helps the defenders to take necessary precautions before the attack occurs.

II. Background

In this chapter, the background of situational awareness, attack graphs and attack trees has been explained briefly.

A. Situational Awareness

Cyber Situational Awareness (CSA) can be described as the traditional Situational Awareness (SA) which is applied to computer networks [9]. The main idea of situational awareness in cyber domain is to analyze the surroundings in cyber domain and creating certain events and visualizations for the purpose of efficient and fast decision making.

Another aim is to prioritize the attacks as all the attacks don't have the same impact over the defended network and system [9]. Hence, the analyst should prioritize the sub-systems and assets first since the impact of attack is determined by the importance of the asset. Then, based on the findings, the critical attacks should be taken into consideration for mitigation planning. It shouldn't be forgotten that the cyber situational awareness of an organization reflects the effectiveness of response to attacks.

According to [10], Situational Awareness for Cyber Defenses includes 7 basic aspects: "Being aware of a. current situation, b. impact of attack, c. how situations evolve, d. actor behavior, e. why and how the current situation is caused, f. quality and how plausible futures of the current situation." Based on this definition, it can be said that situational awareness provides the user the closer view and detailed inspection of network.

Providing the notion of 'situational awareness' will be challenging because of certain rigors in CSA [9]. Firstly, identifying missions will not be so easy that even some organizations don't know their cyber-missions. Moreover, they usually have neither any sufficient tracking mechanisms in their networks nor sensors which will warn them for attacks. Under these circumstances, it is really difficult to have an effective situational awareness. The best solution can be identifying the critical missions which the organization has; then implementing the tracking mechanisms and finally defining proactive solutions for the security of network.

Several studies have been made in this field. While some of the studies [3][10] generally describe the term of situational awareness and standard methods and applications which have been used in order to maintain it; others focus on more specific methods such as real time multistage attack awareness and mission-centric cyber situational awareness [11], [12].

B. Attack Graphs

Attack graphs are valuable analysis results for cyber defense and situational awareness that can map possible paths of attacker who aims to get access by means of infiltrating to a specific network [5]. Attack graphs have multiple capabilities such as [5]:

--network topology creation,
-- understanding baseline behavior in network traffic,
--vulnerability and risk classification,
--more proactive perspective instead of reactive.

Topological Vulnerability Analysis (TVA) is one of the well-known methods that can provide user to monitor the current conditions of network assets and create the models of network vulnerabilities and actual risks [13], [14], [15]. It produces a model by calculating both the individual and combined vulnerabilities. The main output of this security method is the attack graphs which show all the possible paths of an attacker that might infiltrate the network. One of the biggest advantages of TVA is that the raw asset and vulnerability related data gets transformed into meaningful information which shows the possible attacks. By using this information, one can proactively manage risks related to possible attacks and take precautions. If the analyst can do this analysis in real-time, then a just-in-time situational awareness can be achieved.

Recently, new techniques were introduced to visualize attack graphs [16]. The main aim of these attack graphs is to reduce complexity and portray the attack flows in a relatively simple and clear fashion. Attack graph views can be coordinated and the user can have a broader view of the network topology and attack vector [16]. These techniques can be used either independently or in a combined way based on the network complexity. This provides diversity that all has different uses having different properties and perspectives. A brief illustration of the techniques for attack graphs can be found in [16]:

--*Attack Graph Adjacency Matrix Visualization* is used to understand the attack correlation, prediction and association in network attack graphs [17]. It is applied for showing gained access of attacker across the network and predicting all possible paths of the attacker. Based on the collected output, the impact of output is identified and it gives the ability to prioritize attacks according to the impact levels. Adjacency Matrix may be a standalone method as it requires network attack graphs for finding correlations and making predictions [17].

--*Interactive Attack Graph Filtering* is one of the useful methods if the user has larger network. It helps to filter the graph by using a selected schema [16]. Like attack trees, interactive attack graph filtering creates tree widgets to navigate through network. In this way, the user has the chance to focus on the network topology deeply and run through the network step-by-step with the help of penetration testing [16].

C. Attack Trees

Attack trees play a significant role in specifying system security and network in terms of vulnerability and risk identification [18]. They can be mapped in various forms. Mostly, while nodes represent attacks, the root node is the global goal of the attacker which can also described as an event [6]. Child nodes are the refinements of this goal and branches are the attacker's path which cannot be refined anymore. Each path in attack tree represents a unique attack. Moreover, attack trees can also be prepared textually instead of graphically. In textual form, the 'AND' and 'OR' decompositions are used and the consequences of achieve sub-goals were presented by them.

Attack patterns can be defined in order to increase the practicality of attack trees generation and reuse [19]. Attack pattern is the mapping of different types of attacks that

includes a. the goal of the specified attack, b. the preconditions for use, c. the steps for practicing attack, d. postconditions which are true if the attack is made successfully [19]. The preconditions contain assumptions which are related with the expected behaviors of attacker and the characteristics of the attack. The skills, resources, access and knowledge can be given as an example to preconditions [19]. On the other hand, postconditions cover the gained privileges when the attack was resulted successfully.

Attack trees have been used in many various ways and one of the previous studies is related to Supervisory Controls and Data Acquisition (SCADA) protocols [20]. These protocols are communication protocols which are used for exchange of control messages in industrial networks. The use of attack trees for SCADA is based on accessing vulnerabilities and the main purpose is analyzing the measurable goals and structured elaboration of events such as specific attack goals [20]. Like designing the attack patterns in textual way, the study focuses on 'AND' and 'OR' compositions in order to access vulnerabilities.

III. BSGS

In this part, the capabilities, architecture and operational scenario of BSGS and the attack trees generated by the system will be introduced.

A. Capabilities

BSGS integrates and centrally manages vulnerability, network topology and IT assets information collected from the organizational units and backbone network. The prototype calculates the most effective cyber attacks to be carried out by cyber-attackers and attack trees showing the possible attack vectors (vulnerability, topology, etc.) through which they can perform attacks. With the help of the attack tree, BSGS users can calculate the risks inherent in systems and analyse possible remediation.

In addition to the above-mentioned capabilities, BSGS can gather system and application logs and sensor alerts in real time all over the network through a central coordination unit. All collected data are correlated and users are informed by a "Common Operational Picture" that provides cyber situational awareness. It is composed of vulnerability, assets, risks and instant status information such a consolidated cyber security picture allows decision-makers to make integrated risk analysis and corrective action planning.

The developed prototype system has been evaluated in many cyber security scenarios. This evaluation is not only a classic software testing approach; but also the evaluation of effectiveness of the system from the perspective of cyber security experts. As a result of the scenario analysis, it has been evaluated that the competency of BSGS system is within the targeted scope of risk assessment, proactive defense planning, analysis of past cyber action and creation of consolidated cyber security situation picture.

BSGS also benefits from a distributed data processing infrastructure. As a prerequisite, the components, providing the collection of static event and instant event logs, have to be deployed in the organizational unit. Each organizational unit has its own clients and servers and applications running on them and network devices such as IDS, IPS, firewall, etc… Then, this collected information is sent to a coordination center (cyber security operation center). Collected data is merged by using data fusion in order to create an integrated common picture.

BSGS project offers very important gains. With BSGS, foundations of a centre of excellence have been laid. This will be a center where new threats and methods of Cyber Attacks that may arise in the future can be tested and measures can be developed. Thanks to the flexible and scalable technical infrastructure of the BSGS, which has been developed under an R&D project, a long term, easily extendable system has been put into practice. Moreover, a Cyber Security Ontology and National Vulnerability Database have been provided and the infrastructure, which will lead to the formation of the inter-institutional and in-house Cyber Security processes and their coordination structure, has been prepared.

B. Architecture and Operational Scenario

In the following the main sub-systems of BSGS can be found:

--Vulnerability Analysis and Risk Management
--National Vulnerability Database (YZV)
--Attack tree creation infrastructure
--Organizational Cyber Security Application
--Integrated Cyber Security Application
--Central event logger and correlator (SIEM)

Figure 1 illustrates also the main tasks and componens of BSGS.

Fig. 1. BSGS main tasks and components

The operational scenario is as follows:

--Synchronization of vulnerabilities data in NVD (National Vulnerability Database) with local vulnerability database,

--Evaluation of vulnerabilities by analysts,

--Scanning the network topology, asset and vulnerability,

--Collection of static information (the results of scanning) in the coordination center,

--Identification of threat based on assumptions,

--Score and attack tree production based on threats,

--Collection of dynamic information and sending the coordination center,

--Correlation of event logs,

--Visualization of all information collected in the center and creation of integrated cyber security situational awareness common picture. In the following figure, the architecture of BSGS can be found.

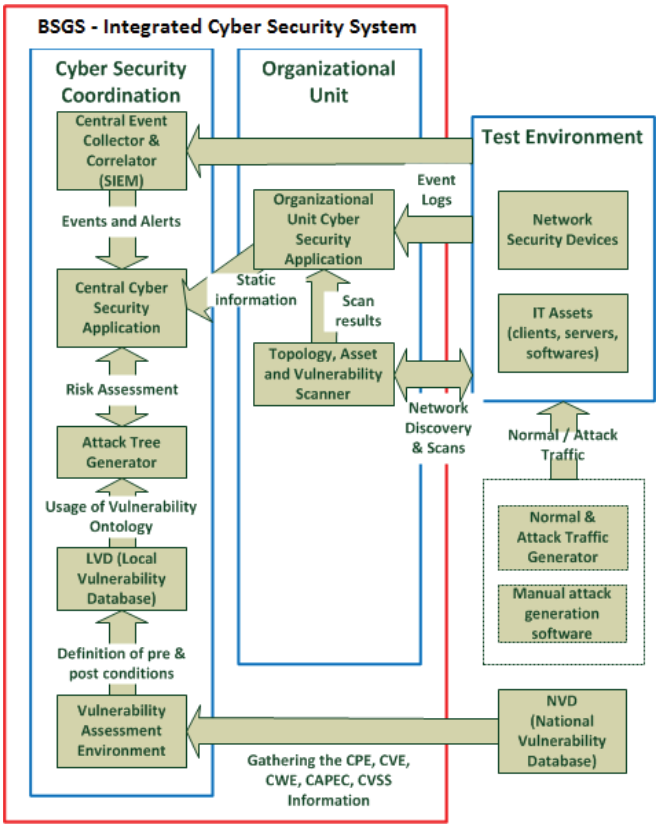


Fig. 2. BSGS is composed of three sub-systems which are cyber security coordination center, organizational unit and test environment

C. *Attack Trees*

The main aim of using attack trees is to find out which types of attacks may be experienced because of critical vulnerabilities and to identify ways of attacks by using assets in the network. Moreover, with the help of attack trees the risks will be calculated and the precautions against attacks will be analyzed and prioritized. In this way, possible risks are identified and arranged in an order based on their risk scores.

While creating attack trees, web ontology language (OWL) is used for discovering the steps (attack tree nodes) and transitions -by using vulnerability- between steps. OWL interpretation requires huge memory and processing power. To overcome this performance bottleneck, attack trees are distributed in parallel fashion. Moreover, instead of creating attack tree by adding the devices one-by-one, the devices which have the same level of accessibility are united and their vulnerabilities are integrated. It is also assumed that possible attacks can affect all clustered devices. In this way, attack trees for very large networks can be processed faster. In the figure 3 and 4,both network and logical topology of the sample system are illustrated. Also, in the figure 5 the illustration of attack tree is shown including the starting point and target system.

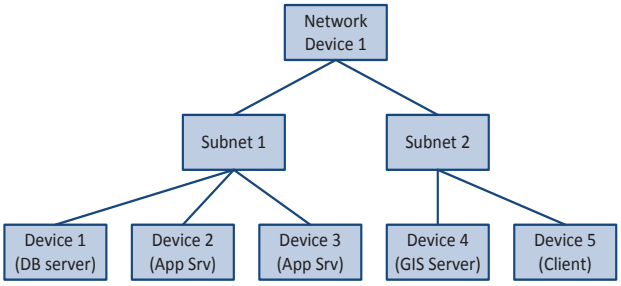


Fig. 3. The network topology of the sample system.

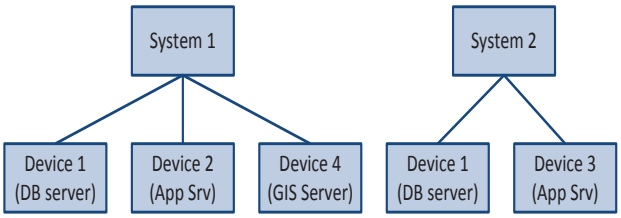


Fig. 4. The sample system's logical topology, showing the business structure of the organization, was illustrated.

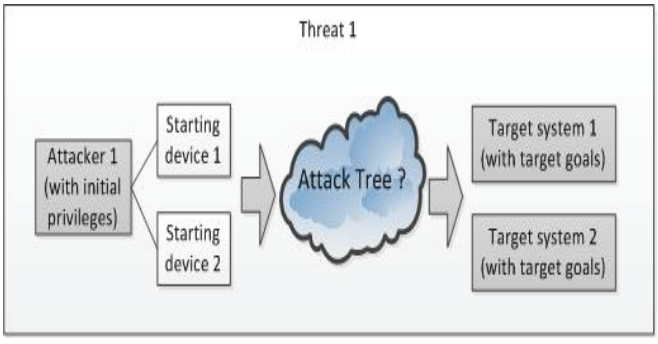


Fig. 5. The main idea of generating attack tree is to show the attacks on a target system where there is an attacker and a starting point (e.g. a compromised device)

The infrastructure of distributed simulation and attack tree gives the possibility of using vulnerabilities coming from local vulnerability database, vulnerability and attack ontology and ontology reasoning engine; then creates the attack tree which

shows the attack paths - which may give harm to system - by evaluating vulnerability preconditions and postconditions. In attack tree, the visualization is based on vulnerabilities. An attack tree node includes a. the device b. vulnerability which is the source of an attack to this device (including pre/post conditions), c. gained privilege as a result of this attack on this device. Afterwards, by using attack trees, impact scores of the vulnerabilities and criticality levels, risk analysis is made and risk scores are calculated for each path in an attack tree. In the appendix, the sample of attack tree can be seen. In figure 6 the necessary input for generating attack tree can be seen in a detailed way.

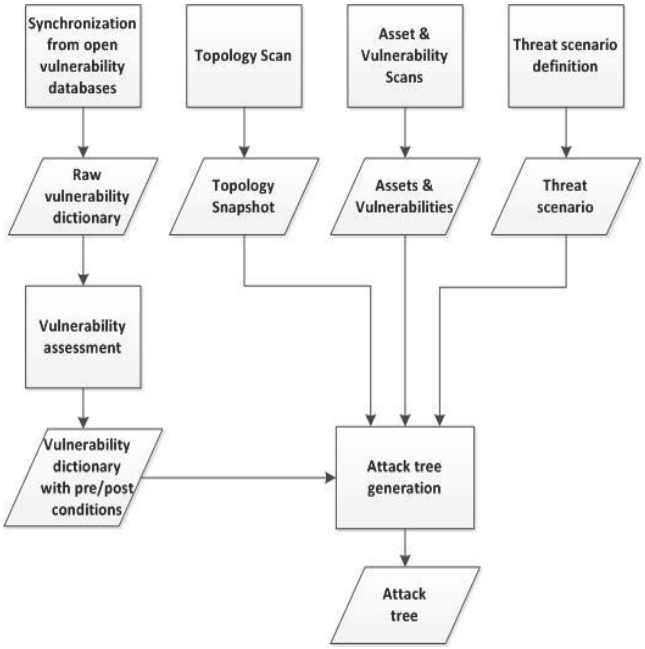


Fig. 6. The collection of vulnerabilities, assets and threats are processed in different ways and then they are all united in attack tree generation process.

IV. Conclusion

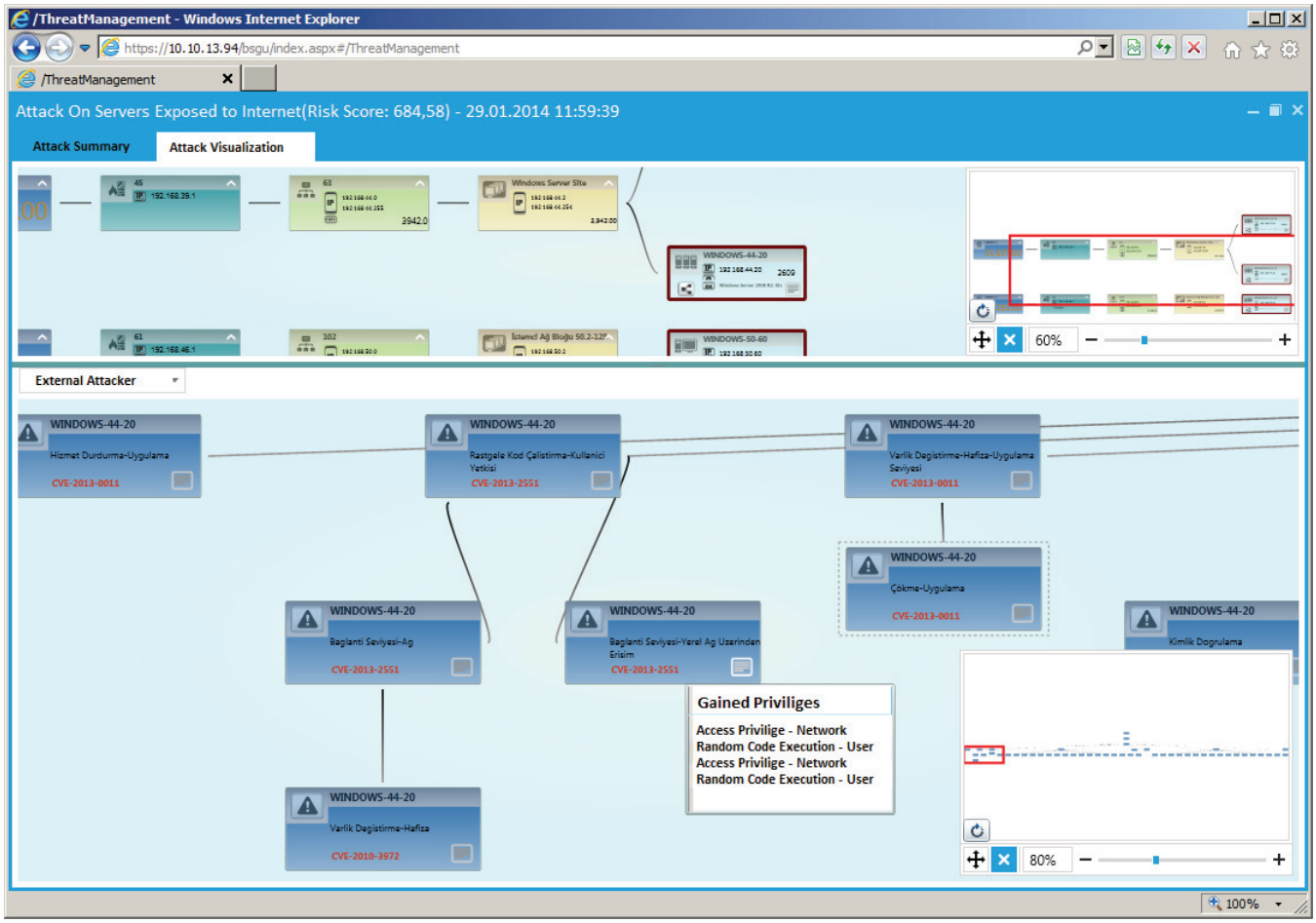
It is certain that the cyber security plays an important role in the protection of IT systems and critical infrastructures. Both proactive and reactive precautions are needed to provide a holistic security approach and situational awareness is essential for making the necessary decisions. Situational awareness is not only used for analyzing the networks and systems; but also needed for fast and accurate decision making. For providing situational awareness in the systems, attack graphs are mainly used to understand baseline behavior of an IT system and detect anomalies in real time. Attack graphs are effective tools which can map possible paths of the attacker through the target source. There are several methods to represent attack graphs as all have different functionalities.

One of them, tree structure, has been used in many ways in IT sector; attack trees provide an effective means of attack visualization in cyber security domain. In this study, an integrated cyber security system, BSGS, is explained as a combination of different cyber security capabilities including attack trees. Attack trees provide a considerable amount of dynamism to the system as it helps users to make risk assessment and management by prioritization. Visualization of such information can help the decision makers to be more efficient and have a higher sense of governance from cyber security perspective.

References

[1] M. Yayla, "Cyber War As A Legal Term," USA, The City University of New York John Jay College, 2013.
[2] *Overview of cybersecurity, ITU-T Telecommunication Standardization Sector Of ITU,* Series X: Data Networks, Open System Communications and Security, Recommendation ITU-T X.1205, 2008 Available: https://www.itu.int/rec/T-REC-X.1205-200804-I.
[3] G. P. Tadda, J. S. Salerno, "Overview of Cyber Situation Awareness," in *Cyber Situational Awareness Issues and Research*, vol. 46, Springer, 2010, pp. 15-35.
[4] D. M. Best, S. Bohn, D. Love, A. Wynne, and W. A. Pike, "Real-time visualization of network behaviors for situational awareness," in *Proc. Seventh International Symposium on Visualization for Cyber Security*, New York, 2010, pp. 79-90.
[5] K. Ingols, R. Lippman, and K. Piwowarski, "Practical Attack Graph Generation for Network Defense," in *Proc. 22th Annual Computer Security Applications Conference(ACSAC'06)*, MIT Lincoln Laboratory 2006, pp. 121-130.
[6] S. Mauw, M. Oostdijk, "Foundations of Attack trees," in *Proc. ISISC 2005 Information Security and Cryptology*, v. 3925, 2006, pp. 186-198.
[7] B. Schneier, "Attack trees: Modeling security threats," Dr. Dobb's journal, 1999.
[8] B. Schneier, "Secrets & Lies: Digital Security in a Networked World," Wiley, 2000.
[9] A. Doupé, M. Egele, B. Caillat, G. Stringhini, G. Yakın, A. Zand, L. Cavedon, and G. Vigna, "Hit'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness," in *Proc. 27th Annual Computer Security Applications Conference*, 2011, pp. 51-61.
[10] L. D. Cumiford, "Situation Awareness for Cyber Defense," *Information for the Defense Community*, 2006.
[11] S. Mathew, D. Britt, R. Giomundo, and S. Upadhyaya, "Real-Time Multistage Attack Awareness Through Enhanced Intrusion Alert Clustering," in *Proc. Military Communications Conference*, 2005, pp. 1801-1806.
[12] S. Jajodia, S. Noel, P. Kalapa, and M. Albanese, "Cauldron mission-centric cyber situational awareness with defense in depth," in *Proc. Military Communications Conference*, 2011, pp. 1339-1344.
[13] S. Jajodia and S. Noel, "Topological Vulnerability Analysis," in *Cyber Situational Awareness Advances in Information Security*, v. 46, Springer, 2010, pp. 139-154.
[14] S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis of Network Attack Vulnerability," in *Managing Cyber Threats: Issues, Approaches and Challenges*, v. 46, Springer, 2005, pp.247-266.
[15] S. Jajodia and S. Noel, "Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response", in *Proc. Algorithms, Architectures and Information System Security*, New Jersey, 2009, pp. 285-305.
[16] S. Noel, M. Jacobs, P. Kalapa, and S. Japodia, "Multiple Coordinated Views for Network Attack Graphs," in *Proc. IEEE Workshop on Visualization for Computer Security*, 2005, pp. 99-106.
[17] S. Noel, "Understanding complex network attack graphs through clustered adjacency matrices," in *Proc. 21st Annual Computer Security Applications Conference*, 2005, pp. 10-169.
[18] I. Ray and N. Poolsapassit, "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders," in *Proc. Computer Security - ESORICS 2005 Lecture Notes in Computer Science*, v. 3679, 2005, pp. 231-246.
[19] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack Modeling for Information Security and Survivability," Carnegie Mellon Software Engineering Institute, 2001.
[20] E. J. Byres, M. Franz, and D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems," in *Proc. International Infrastructure Survivability Workshop (IISW'04)*, Institute of Electrical and Electronics Engineers, Lisbon, 2004.

APPENDIX


/ThreatManagement - Windows Internet Explorer
https://10.10.13.94/bsgu/index.aspx#/ThreatManagement
/ThreatManagement
Attack On Servers Exposed to Internet(Risk Score: 684,58) - 29.01.2014 11:59:39
Attack Summary
Attack Visualization
External Attacker
WINDOWS-44-20
Hizmet Durdurma-Uygulama
CVE-2013-0011
WINDOWS-44-20
Rastgele Kod Çalistirma-Kullanici Yetkisi
CVE-2013-2551
WINDOWS-44-20
Varlik Degistirme-Hafiza-Uygulama Seviyesi
CVE-2013-0011
WINDOWS-44-20
Çökme-Uygulama
CVE-2013-0011
WINDOWS-44-20
Kimlik Dogrulama
WINDOWS-44-20
Baglanti Seviyesi-Ag
CVE-2013-2551
WINDOWS-44-20
Baglanti Seviyesi-Yerel Ag Üzerinden Erisim
CVE-2013-2551
Gained Priviliges
Access Privilige - Network
Random Code Execution - User
Access Privilige - Network
Random Code Execution - User
WINDOWS-44-20
Varlik Degistirme-Hafiza
CVE-2010-3972
60%
80%
100%