International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-2, February 2016

New Modeling Technique for Detecting, Analyzing, and Mitigating Multi Attacks

Adel E. Gomaa, Adly S. TagEldien, Tarek EL-Shishtawy

***Abstract*— With the expansion in depending on computer networks, the risk of network attacks are raised, therefore, there is an increasingly need for model helping the network administrator to detect vulnerabilities, attacks scenarios, and mitigate vulnerabilities. While source and timing of attacks can't be predicted, their impact can be reduced by knowing the possible attack scenarios through network. Manual processes and mental models can't be trusted, and there is a need for new model to secure, analyze, and visualize vulnerability dependencies of enterprise networks. This is helps understanding the overall security posture, and providing context over the full security life cycle. In this paper, proposed a novel model for enterprise networks security which are modeled network topology, configuration, multi-credential theft, and access attacks. The proposed model adopts a high level of abstraction for specifying network configurations and topologies and does not rely on specific protocols and standards. The model is verified by predicting different attacks scenarios. Also, the model is useful in predicting suitable techniques for mitigating attacks. Moreover, the intrusion perversion system, and unified threats management filtering rules can be modeled and analyzed to determine the initial accesses in the network. Furthermore, a tool is implemented using an expert system based on proposed model to analyze network configurations and detect how an attacker may exploit chain of vulnerabilities to reach his goal and attack multi-hosts at the same time is very useful. Network administrator can use the tool to explore all attacking paths and generates the closure of access rights that the attacker can gain by exploiting the vulnerabilities. Finally, a case study is also presented to explore the tool applicability and show its efficiency and flexibility.**

***Index Terms*— expert system, mitigate attacks, multi-attacks scenarios, network security, and network vulnerability**.

I. INTRODUCTION

Network vulnerabilities refer to the weaknesses of a target system network [1], for examples, security flaws in server software (e.g., Apache Chunked-Code software, Oracle and TNS Listener software) or network configurations (e.g., enabled ports and services). Vulnerability can be exploited when its pre-conditions are satisfied. These pre-conditions include network connectivity, user access privileges on relevant hosts, and network or host configurations. Vulnerability exploit usually deals with two hosts: an attacking host (the source host on which an attacker performs an exploit), and a victim host (the destination host on which an attacker gains benefits after the exploit has been accomplished). There are two exploit modes: local and remote. For the local exploit mode, vulnerability can only be exploited at the victim host. For the remote exploit mode, the vulnerability can be exploited at either host (i.e., the attacking and victim hosts can be the same or different). Attackers can combine vulnerabilities in unexpected ways and compromise critical systems. Protecting critical infrastructure networks need to understand not only individual systems vulnerabilities, but also their interdependencies. Each machine's susceptibility to attack depends on the vulnerabilities of the other machines in the network. This is compounded by the fact that each machine's exposure to attack depends on the vulnerabilities of the other machines in the network. In order to secure network, network administrators need to know existing vulnerabilities, multi-attacks scenarios that may be take place in their networks [2, 3], and suitable techniques for mitigating attack. Many approaches [4-14] are proposed to analyze network vulnerabilities from the point of view of the relations between individual hosts and network. Such approaches mainly used model checking and graph-based techniques to generate and analyze an attack graph; they used model checking such as SMV [15] to predict attacks scenarios, when model checker result is counter example, this is meaning there is one attack path, so, every counter example represented attack path.

Other approach [16] is proposed a general framework for modeling typical network topologies, and configurations. The topological part describes the structure and how components are connected. The configuration part describes routes of the packets through network, users' privileges, and how users access network. This model uses a high level of abstraction, it isn't depended on protocol or topology, and it is considered firewall rule filter. Also, the approach is modeled vulnerabilities depending on preconditions and post-conditions, it is modeled some vulnerabilities such as usurp, local program, and denial of services. Then the approach showed how an expert system can be implemented based on this framework for automating the process of multi-host vulnerability analysis. This approach is used network scanner tool such as Nussus [17] to discover vulnerabilities in network and model checker NuSMV [15] to predict all attacks paths. Some approaches [20, 21] are proposed predictive model using artificial intelligence to detect and classify attack type for Intrusion Detection System (IDS).

Network attacks mitigation techniques [22, 23, 24] are proposed to implement mitigations to credential theft attacks. The recommended mitigations are intended to help network administrator significantly minimize the risk and impact of attacks and other credential theft attacks in his organization.

In this paper, we extended a model that is proposed in [16] to describe network topology, configuration, and different types

Adel E. Gomaa, Ccmputer engineering department ,Shoubra Faculty of Engineering, Benha University, Cairo, Egypt.

Adly S. TagEldien, **,** Ccmputer engineering department ,Shoubra Faculty of Engineering, Benha University, Cairo, Egypt

Tarek EL-Shishtawy, Faculty of Computers and Informatics, Benha University, Egypt.

of attacks. The novel model can predict multi- attacks scenarios and the process of attacks mitigation. Novel model concerned with two types of attacks: the first is access attacks which are include password attack, man-in-the middle, and trust attacks; the second is credential attacks which are include DDos (Distribution Denial of Service), privacy forfeit, and Entirety Forfeit attacks. Apply the model is explored the multi-attacks scenarios that used by attacker. The proposed model is efficient as well as flexible enough to address most of the wide-spread attacks methods and mitigation techniques. Additionally the DDoS attack which may interrupt a service or access on many hosts at the same time is represented and analyzed in the proposed model. Moreover, in the proposed model, the topology of the network is represented and analyzed to obtain the initial accesses of principals in the network. Also, Unified Threat Management (UTM), and Intrusion Prevention System (IPS) are modeled and analyzed by this model. Furthermore, redesign network become easy by using proposed model because the network administrator can simulate new design and test for minimizing vulnerabilities before applied on network. An expert system is implemented based on the proposed model for automating the process of multi-host attack analysis. Finally, our system has broad range of applications in design of secure networks. It also provides assistance in tracing security requirements and expert guidance through the full design cycle.

The remaining of this paper is organized as follows: Section2, related work is discussed. Section 3 deals with model of network topology, and configuration. Also section 3 deals with modeling different types of attacks, mitigation, and detecting multi-attacks scenarios. In section 4 the model is applied on a network as a case study. Finally, the last section underlines some concluding regards.

II. Related work

Attackers look for network vulnerabilities which can be exploited when their pre-conditions are satisfied. To predict attacks scenarios, pre-conditions and post- conditions of network should be known, (i.e., transition states of network), so, some researchers [25, 26, 29, 30] viewed network as a graph, each graph consists of nodes (represent network devices) and arcs (represent links connectivity), and they used graph theory that determine transitions states' of network under attack to construct attack graph or scenario which represents different ways in which an intruder may reach a certain goal such as root access on a host. Attack scenarios produced manually by Red Teams [31], which are ponderous, complex, and impractical for large network which have a hundred nodes. The NetKuang system [4] which is rule based expert system for checking the security of computer network that is used Unix operating system and can find vulnerabilities created by poor system configuration. NetKuang analyzes the systems on which it is running to determine if the initial privileges are enough to obtain the target privileges. Although it was the first work tried to detect multi- attacks, it was limited to some vulnerabilities of UNIX configuration. This approach has been adopted and scrutinized by [6-11] that are analyzed network vulnerabilities for generating attack graph which is used to predict multi attacks scenarios. In their approach, attacks are modeled as pre-conditions and post-conditions and a specific tool such as Graph Viz [32] has been used to construct the attack graph. Although the algorithm is effective, but, deal with each attack individually resulted in a large and complex model, and the role of firewalls was not considered. The firewalls and some kinds of vulnerabilities are considered in [16] but, Unified Threat Management (UTM), and Intrusion Prevention System (IPS) was not considered. This is not all, the credentials theft attacks were not considered, and mitigation techniques also. So, we proposed model for covering all of these subjects. Rule based systems have been used in the area of network security at Intrusion Detection or Prevention mainly, such as [18, 19, 20, 21]. In these approaches, rule based system is used to reason about the security state of the system, given rules that describe intrusive behavior. We use rule based system based on proposed model for specifying multi-attacks scenarios on multi-hosts in the network at the same time and mitigation techniques. Our rule based system uses forward chaining algorithm and starting from the initial state, and it finds new facts that can be derived from initial facts by applying production rules.

III. Modeling Attacks and Detect Attacks Scenarios

Model which proposed in [16] will be extended. This model has been modeled network, internetwork connection, network access, firewall rules, and router. Also, it is modeled some vulnerabilities depending on preconditions and post-conditions, such as usurp, local program, and denial of services. We will be considering IPS, UTM, access attack, and credential theft attacks.

A. Modeling IPS

- IPSRule (ips, SH, DH, a, Sign):

This fact defines a filtering rule in Intrusion Prevention System (IPS) for packets with source host (SH), destination host (DH), and internal signature (Sign)

sh ∈ SH, dp ∈ DP, and dh ∈ DH, and sign ∉ Signatures, then this rule cause action (a) to be done on accesses.

- PacketCanPass(ips, h, h', Sign):

The configuration of IPS (ips) pass packets with source host (h), destination host (h'), and source packet is not one of internal signature of IPS.

B. Modeling UTM

Unified Threat Management (UTM) is a solution in the network security industry, and it has gained currency as a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance: network firewall, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, Virtual Private Network (VPN), content filtering, load balancing, data leak prevention and on-appliance reporting. We are concentrating on two functions: firewall, and IPS. We define a rule for these functions

- UTMRule (utm, SH, DH, DP, Sign, pr, a):

This fact defines a filtering rule in Unified Threat Management (UTM) for packets with source host (SH),

destination host (DH), destination port (DP), internal signature (Sign), and the priority of this rule is (pr).

Suppose sh ∈ SH, dp ∈ DP, and dh ∈ DH, and sign ∉ Signatures, then this rule causes action (a) to be done on accesses from host (sh) to port (dp) of host (dh), providing that there is no other rule with higher priority matched with the packet. The action (a) can be either permit or deny and the priority of this rule is (PR).

- PacketCanPass(utm, h, h',p, Sign):

The configuration of UTM (utm) pass packets with source host (h), destination host (h'), destination port (p), and source packet is not one of internal signature of UTM.

`

C. Access Attacks and Mitigation Techniques

Access attacks include three types: password attacks, trust exploitation, and man-in-the-middle attacks.

1) Modeling Password Attacks

Password attacks can be implemented using several methods such as brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. When an attacker gains access to a resource, the attacker has the same access rights as the users whose accounts have been compromised. If these accounts have sufficient privileges, the attacker can create a point for future reentry, or a "back door" for future access, without concern for any status and password change to the compromised user account. An example that compromises network integrity is when an attacker modifies the routing tables for the network. By doing so, the attacker ensures that all network packets are routed to the attacker before they are transmitted to their final destination, in such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle. In fact, when a user has access to one account on a host, he can find all of the other accounts on this host. After finding all of the accounts on a host, the attacker can guess the password of those accounts on this host. Another form of this attack happens when a host offers services like Telnet and SSH that users can use to have a remote login to a host. An attacker (a') which knows there is user account (a) on this host (h) (e.g. using social engineering methods) can use a dictionary attack to find the password of this account. Models of these classes of attack are as follows:

Attack LocalPassword
Preconditions:
Priv(u, a, h)
Account(a′, h)
Password(a, h)
Postconditions:
Priv(u, a′, h)

Attack RemotePassword
Preconditions:
Social engineering(a′,a)
NetworkAccess(u,p,h)
Password(a, h)
RemotPasswordAuth(p)
Priv(u, a, h)
Postconditions:
Priv(u, a′, h)

Password attack mitigation techniques are as follows:

- Prevent users from using the same password on multiple systems. Most users use the same password for each system they access, and often personal system passwords are also the same.
- Disable accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
- Prevent plain- text passwords. Allowing either an OTP (One Time Password) or encrypted password.
- Force users to use strong passwords, many systems now provide strong password support.

2) Modeling Trust Attack

Although it is not an attack in itself, "trust exploitation" refers to an individual taking advantage of a trust relationship within a network. For example, trust exploitation may occur in the following scenario: a system outside the firewall has a trust relationship with a system inside the firewall. When the outside system is compromised, the attacker can leverage that trust relationship to attack the network inside. Suppose that Trust host *(h')* can connect with host *(h)* and user *(u)* has privileges of account *(a)*. If attacker *(a')* can be accessed trust host *(h')*, then attacker *(a')* can be exploited host *(h)* and run his code on that host with privileges of account *(a)*:

Attack Trust
Preconditions:
Priv(u, a, h)
TrustAttack(h, h')
Account(a', h')
Postconditions:
Priv(u, a', h)

You can mitigate trust exploitation- based attacks through employing tight constraints on trust levels within a network. Systems outside the firewall should never be absolutely trusted by systems inside the firewall. Such trust should be limited to specific protocol and, where possible, should be validated by something other than an IP address.

3) Modeling Man-in-Middle Attack

An example of a man-in-the- middle attack occurs when someone working for your ISP (Internet Service Provider) gains access to all network packets transferred between your network and any other network. Man-in-the-middle attackers take care not to disrupt traffic and thus set off alarms. Instead, they use their positions to stealthily extract information from the network. In this class of attack, there is a root user *(u)* that consider administrator, with the privileges of account *(a)* on host *(h)* which can be accessed network resources and there is an attacker *(a')* can be captured outgoing and incoming traffic of network, then attacker *(a')* can access network with administrator privileges, this show in the following model:

Attack man-in-middle
Preconditions:
Priv(u, a, h)
NetworkAccess(u,p,h)
Man-in-middleAttack(a', h)
Postconditions:
Priv (u,a',h)

Man-in-the-middle attack mitigation is achieved by encrypting traffic in an IPSec tunnel. Encryption allows the attacker to see only cipher text.

D. Modeling Credential Theft Attacks

Credentials include anything used to identify and authenticate a user or device [26]. An attacker who is able to obtain a valid set of credentials (like a username and its associated password) can simply use them to gain access to systems [25]. In this kind of attack two steps are taken by attackers escalate privileges, and move laterally involves the theft and subsequent use of stolen credentials. Underhere modeling some types of credential theft attacks.

1) Modeling Privacy Forfeit Attack

In this class of attacks, an attacker (a') that was not allowed to read some privacy data has got privileges of a new user account (a) that is authorized to read these data. Therefore although the attacker is not the legal owner of account (a), he can use the privileges of this account and read these privacy data:

Attack privacyforfeit
Preconditions:
Priv(*A*, *a*, *h*)
CanReadprivacyData(*a*, *h*, *path*)
AccountOwner(*A*, *a*, *h*)
¬ *AccountOwner*(*A*, *a'*, *h*)
Priv(*A*, *a'*, *h*)
Postconditions:
privacyforfeit (*a'*, *h*, *path*)

2) Modeling Entirety Forfeit Attack

In this class of attacks, an attacker (a') that was not allowed to modify some data has got privileges of a new user account (a) that is authorized to modify these data. Therefore although the attacker is not the legal owner of account (a), he can use the privileges of this account and modify these privacy data:

Attack EntiretyForfeit
Preconditions:
Priv(A, a, h)
CanModifyData(a, h, path)
AccountOwner(A, a, h)
¬ AccountOwner(A, a', h)
Priv(A, a', h)
Postconditions:
EntiretyForfeit (a', h, path)

3) Modeling Distribution Denial -of -Service Attack

This type of attack consists of two levels [27]. The first level is Low rate distributed denial of service (LR-DDoS) attack which is an intelligent attack that saturates the victim with packets adequately in low rate, in order to avoid the current anomaly based detection schemes. LRDDoS attack is widely used in a large sizeDDoS attack, which joins several low rate attacks [28], LR-DDoS attack produces network traffic similar to the normal network traffic, and, therefore, it is difficult to be detected and mitigated. The second level is high rate distributed denial of service (HR-DDoS) attack which is a synonym for the traditional DDoS attacks when attackers exceed and violate the adopted threshold value.

In this kind of attacks, different services that are running on more than one host are vulnerable to some patterns of data. Attackers that have access to one of these hosts can exploit these vulnerabilities and prevent services from responding to requests:

Attack *DDoS*
Preconditions:
Service(s_s, *p*, *a*, h_h)
NetworkAccess(*A*, *h*, *p*)
DDoSAttack(s_s, h_h)
Postconditions:
¬ *Service*(s_s, *p*, *a*, h_h)
Where: {s(1,…..,n), h(1,….,n)}

E. Mitigation Credential Theft Attacks

Techniques to mitigate the risk of credential theft attacks tend to be focused on reducing the instances of credentials to steal, reducing the ability for attackers to gain administrative rights, reducing the ability for attackers to utilize stolen credentials, and comprehensive prevention that address the attack problem before, and during an actual attack [33-34]. The first method is to minimize administrative rights. This means to limit the number of users with administrative rights to clients and servers, limit the number of other local administrative accounts, as well as limit the number of accounts with domain admin (or similarly privileged) access. This reduces the number of accounts that can be used by attackers to steal credentials from systems across the organization, and reduces the number of highly privileged accounts that attackers often target. Not only should the number of accounts be reduced, but accounts granted increased privileges should be given only the minimum necessary. The next method is to restrict local accounts on clients from being able to access the client over the network. The third method is to minimize the number of shared passwords across multiple systems and accounts. In the event that a local administrative account must exist across many systems and allow access over the network, the password for the account on each system should be different. The fourth technique is network isolation. This can be as simple as setting the firewall on clients to deny incoming connections (except from known management servers, potentially). Lastly, the ideal control is not allowing systems to get compromised in the first place, not allowing untrusted users to gain local administrative rights to any system, and prevent suspect customers from generating flooding attacks.

F. Building Rule-based System

Rule based system is based on the proposed model introduced in the previous sections for automatic detecting, analysis, and mitigating network multi-attacks. This rule based system consists of four main components: Multi- Attacks Scenarios Model, Expertise of Attacks Mitigation (Knowledge Base), Inference Engine, and User Interface as shown in Fig.1

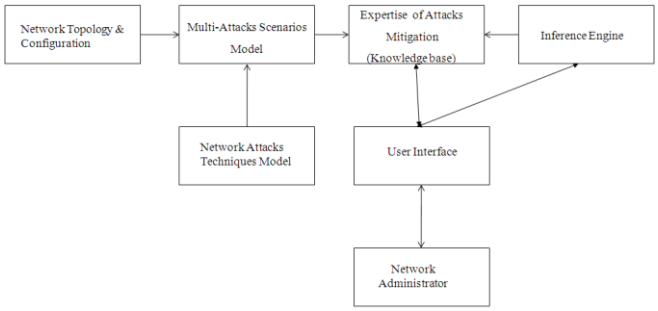

Fig.1 Expert System Architecture

There are two other components, one of them is Network Topology and configuration and the other is Network Attacks Techniques Model. System algorithm as shown in fig.2 which is illustrated system work cycle

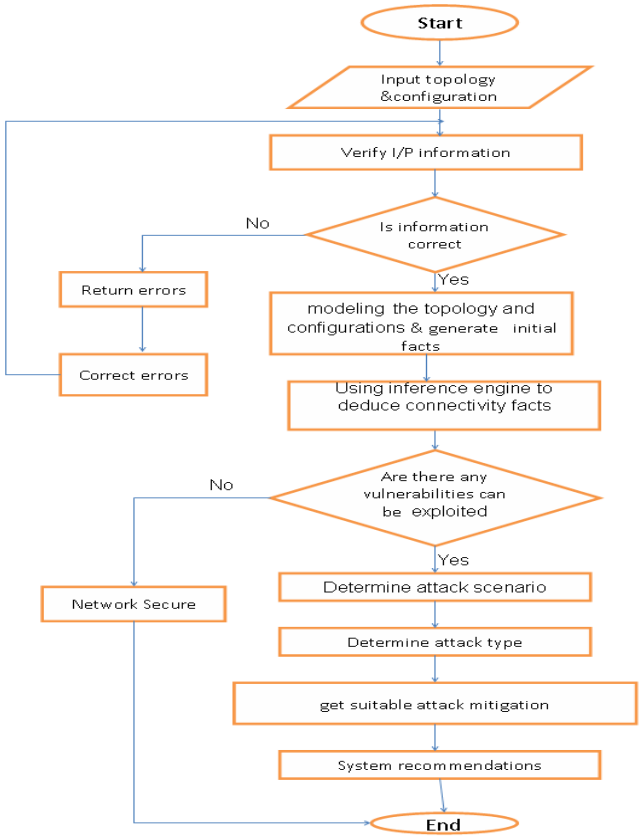

Fig.2 System Algorithm

Knowledge Base is the collection of facts and inference rules that were introduced in the previous sections. Inference Engine is the processing unit that makes logical inferences on the facts and rules that are stored in the knowledge base. User Interface controls the inference engine and manages inputs and outputs. Network topology and configuration is specified initial facts of network such as network components names', connection between network components,…ects. Network attacks techniques model is modeled different kinds techniques of attacks as mentioned before. Multi-attacks Scenarios Model is received the output of network topology, configuration, and attacks techniques model and applied the proposed model to predicts attacks scenarios and path of them to pass the results to knowledge base which is reacted with inference engine to inference suitable mitigation techniques for reducing risk of attacks.

We used the matured expert system tool CLIPS [35] for reducing the amount of time required for developing the expert system. CLIP is called an expert system tool because it is a complete environment for developing expert systems which includes features such as an integrated editor and a debugging tool. The word shell is reserved for that portion of CLIPS which performs inferences or reasoning. The CLIPS shell provides the basic elements of an expert system:

1.Fact-list, and instance-list: Global memory for data
2. Knowledge-base: Contains all the rules, the rule-base
3. Inference engine: Controls overall execution of rules.

A program written in CLIPS may consist of rules, facts, and objects. The inference engine decides which rules should be executed and when. A rule-based expert system written in CLIPS is a data-driven program where the facts, and objects if desired, are the data that stimulate execution via the inference engine. There are three ways to represent knowledge in CLIPS:

- Rules, which are primarily intended for heuristic knowledge based on experience.
- Deffunctions and generic functions, which are primarily intended for procedural knowledge.
- Object-oriented programming, also primarily intended for procedural knowledge.

G. Case Study

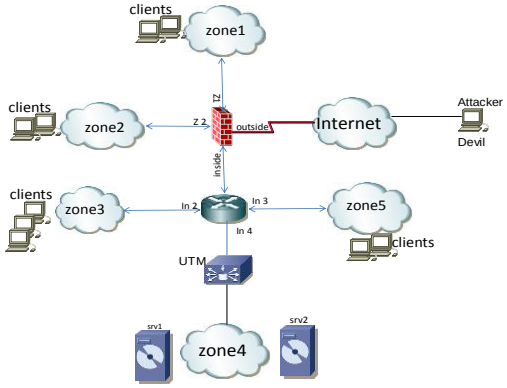

Fig. 3 Sample network

To apply our model we need to document network as shown underhere:

Zones

No.	Zones Name
1	Zone1
2	Zone2
3	Zone3
4	Zone4
5	Zone5
6	Internet
7	ZoneBB
8	ZoneUTM

services

No.	Host Name	Zone Name	Names of Users Accounts	privileges				Types		
				R	W	D	E	admin	standard	Offered Services
1	DC_SRV	Zone 4	Administrator	X	X	X	x	x	-	RPC SSH
2	Db_SRV	Zone 4	Administrator	X	X	X	x	x	-	Oracle db
3	Mail_SRV	Zone 4	Administrators	X	X	X	x	x	-	Stmp
4	Web_SRV	Zone 4	Administrator	X	X	X	x	x	-	http ftp
5	Clin1: clin48	Zone 1	account 1	x	-	-	-	-	X	-
6	Clin500:clin1000	Zone 2	account 500	x	-	-	-	-	X	-
7	Clin96: clin191	Zone 3	account 96	x	-	-	-	-	X	-
8	Clin192: clin239	Zone 5	account 192	x	-	-	-	-	X	-
9	Visitors or attackers	internet	administrator	x	-	-	-	-	-	-

Users

Name of User Accounts	Host Name	Owner name	Groups Names	Password	
				Complex	normal
User1_DC_srv	DC-srv	administrator	administrator	X	-
User2_DC_srv		administrator	administrator	X	-
User3_DC_srv		operator	operator	X	-
User4_Db_srv	Db_srv	administrator	administrator	X	-
User5_Db_srv		User	user	X	-
User6_ Mail_srv	Mail_srv	administrator	administrator	X	-
User7_ Mail_srv		operator	operator	X	-
User8_ Web_srv	Web_srv	administrator	administrator	X	-
User9_ Web_srv		operator	operator	X	-
User1_clin1:	Clin1:	User	user	X	-
user48_clin48	clin48				
User500_clin500: user1000_clin1000	Clin500:clin1000	User	user	X	-
User1_clin96: user191_clin191	Clin96:clin191	User	user	X	-
User192_clin192: user239_clin239	Clin192: clin239	User	user	X	-

Services

No.	Service Name	Host Name	Groups of user Account	Port
1	HTTP	Web_srv	Administrator	http
2	FTP	Web_srv	Administrator	ftp
3	SMTP	Mail_srv	Administrator	smtp
4	RPC	DC_srv	Administrator	rpc
5	SSH	DC_srv	Administrator	ssh
6	ORACLE_DB	DB_SRV	Administrator	Db_port

Gateways

No.	Gateway Name	Type			No. of interfaces	No. of Rules filtering
		R	FW	IPS		
1	BB	x	-	-	4	-
2	FW	-	x	-	4	
3	UTM			x	2	

Firewall

Firewall Name	No. of interfaces	Name of Interfaces	Connected to Zones/Gateway
FW	4	Outside	Internet
		Inside	zoneBB
		Z1	Zone1
		Z2	Zone2

Rule No.	Source Host	Desten. Host	Desten. Port	priority	Action	
					P	D

0	AnyHost	WEB_SRV	http	0	x	-
1	AnyHost	MAIL_SRV	stmp	1	X	-
2	AnyHost	DB_SRV	Db_port	2	x	-
3	AnyHost	devil	http	3	x	-
4	AnyHost	devil	stmp	4	x	-
5	AnyHost	DC_srv	AnyPort	7	x	-
6	AnyHost	DC_srv	ssh	8	x	-
7	AnyHost	AnyHost	AnyPort	10	-	x

Unified Threats Management (UTM)

No.	UTM Name	No. of interfaces	Name of Interfaces	Connected Zones
1	UTM	2	In	zoneBB
			Out	Zone4

Rule No.	Source Host	Desten. Host	Signature		Action	
			Same	Diff.	P	D
0	Any	Zone4 (All hosts)	X	-	-	x
1	any	Zone4 (All hosts)	-	X	X	-

Defined the network documentations to the proposed model:
The network security Expert System

to use this system you have to enter the topology of the network
by defining the zones,, hosts,services,gatewayes,interfac, filtering rules
Do you want to start entering the topolopgy now (yes/no)? y
enter the number of zones in the network :
8
enter the zone name1
zone1
Enter the zone 1 type (local/internet) local
enter the number of hosts in zone :zone1
1
enter the host name1
client1
Enter the number of user accounts in host :client1
1
Enter the user account1 on host client1
account1

According to previous network definitions, the proposed model described network initial states (network topology and configuration) as the following:

f-956 (BetweenZones FW zoneBB internet)
f-957 (BetweenZones UTM zoneUTM internet)
f-958 (BetweenZones FW zoneUTM internet)
f-959 (BetweenZones UTM zoneBB internet)
f-960 (BetweenZones FW zoneBB zone2)
f-961 (BetweenZones UTM zoneUTM zone2)
f-962 (BetweenZones FW zoneUTM zone2)
f-963 (BetweenZones UTM zoneBB zone2)
f-964 (BetweenZones FW zoneBB zone1)
f-965 (BetweenZones UTM zoneUTM zone1)
f-966 (BetweenZones FW zoneUTM zone1)
f-967 (BetweenZones UTM zoneBB zone1)
f-968 (BetweenZones FW zone1 zoneBB)
f-969 (BetweenZones FW zone1 zone2)
f-970 (BetweenZones UTM zone1 zone2)
f-971 (BetweenZones FW zone1 internet)
f-972 (BetweenZones UTM zone1 internet)
f-973 (BetweenZones FW zone1 zoneUTM)

Applying propose model to detect multi-attacks scenarios according to network topology and configuration as illustrate:
There is a Entirety forfeit attack
User user8_Web_srv can use the privileges of account administrator
that is authorized to modify privacy data to modify this data on host Mail_SRV
Entirety for feit attack mitigation :
1- limit the number of users with administrative rights to clients and servers,
limit the number of other local administrative accounts, and limit the number of accounts with domain admin (or similarly privileged) access.
2- restrict local accounts on clients from being able to access the client over the network.
3- minimize the number of shared passwords across multiple systems and accounts
4- network isolation by setting the firewall on clients to deny incoming connections except from known management server

IV. Conclusion

The issue of securing the network is haunt various organizations due to the dependency of these organizations on computer networks, preparing specialists in the field of securing networks takes a lot of time, high cost, and also network security equipments vary from vendor to another, so the proposed model reveal to the network administrator how to predict attack scenario and mitigate, irrespective of standard network topologies, used network protocols, brands, and network components. Also, modeling of new network components such as IPS, UTM, main- in the middle attack, trust attack, Distribution Denial of Service (DDoS) attack, Privacy Forfeit Attack, and Entirety Forfeit Attack have been missed in the previous models. Finally, we have been implemented an expert tool, this tool predicting multi-attacks scenarios and recommend suitable mitigation techniques according to attack type.

Reference

[1] R.Albert, and A-L. Barabási, "Topology of evolving networks: local events and universality", Physical Review Letters, no. 85, pp. 5234, 2000.
[2] Hiran V. Nath, "Vulnerability Assessment Methods - A Review", 4th International Conference, India, 2011, Advances in Network Security and Applications, Proceedings, pp 1-10
[3] Ju An Wang, Minzhe Guo, Hao Wang, Linfeng Zhou "Measuring and ranking attacks based on vulnerability Analysis". Springer-Verlag, 2012, pp 455-490

[4] D. Zerkle and K. Levitt, "NetKuang – A multi-host configuration vulnerability checker," in Proceedings of the 6th USENIX Security Symposium, 1996, pp. 195-204.
[5] M. Dacier and Y. Deswarte, "Privilege graph: an extension to the typed access matrix model," in Proceedings of the 3rd European Symposium on Research in Computer Security, LNCS 875, 1994, pp. 319-334.
[6] R.W. Ritchey, P. Ammann "Using Model Checking to Analyze Network Vulnerabilities". Proceedings of IEEE Symposium on Security and Privacy, pages 156–165, May 2001.
[7] C. R. Ramakrishnan and R. Sekar, "Model-based analysis of configuration vulnerabilities," Journal of Computer Security, Vol. 10, 2002, pp. 189-209.
[8] H. R. Shahriari and R. Jalili, "Using CSP to model and analyze transmission control protocol vulnerabilities within the broadcast network," in Proceedings of the IEEE International Networking and Communication Conference, 2004, pp. 42-47.
[9] P. Ammann, D. Wijesekera, S. Kaushik "Scalable Graph-Based Network Vulnerability Analysis." Proceedings of 9th ACM Conference on Computer and Communications Security, , 2002, pp. 217-224.
[10] L. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer attack graph generation tool," in Proceedings of DARPA Information Survivability Conference & Exposition II, 2001, pp. 307-312.
[11] S. Jajodia, S. Noel, and B. O'Berry, "Managing cyber threats: issues, approaches and challenges. Topological Analysis of Network Attack Vulnerability." Kluwer Academic Publisher, 2005.
[12] Steven Noel, Eric Robertson. "Correlating Intrusion Events and Building Attack Scenarios Through Attack Graph Distances". Computer Security Applications Conference, 2004. 20th Annual. IEEE, pp 350-359. .
[13] H. R. Shahriari, R. Sadoddin, R. Jalili, R. Zakeri, and A. Omidian, "Network vulnerability analysis through vulnerability take-grant model (VTG)," in Proceedings of the 7th International Conference on Information and Communications Security, LNCS 3783, 2005, pp. 256-268.
[14] Hasmik Sahakyan, Daryoush Alipour, "On Attack Graph Model of Network Security," International Journal "Information Content and Processing", Volume 2, Number 1, 2015.
[15] NuSMV. NuSMV: Anew symbolic model checker". http://afrodite.itc.it:1024/nusmv/
[16] Hamid Reza, Yasser Ganjisaffar, Rasool Jalili, and Jafar Habibi, "Topological Analysis of Multi-phase Attacks Using Expert Systems". Journal of InformationOScience and Engineering 24, IEEE, 2008, pp 743-767.
[17] http://www.tenable.com/products/nessus
[18] T. F. Lunt and R. Jagannathan, "A prototype real-time intrusion-detection expert system," in Proceedings of IEEE Symposium on Security and Privacy, 1988, p. 59.
[19] A. Mounji, "Languages and tools for rule-based distributed intrusion detection," Ph.D. Dissertation, Facultés Universitaires Notre-Dame de la Paix Namur, Belgium, 1997.
[20] Roshani Gaidhane, C. Vaidya, "Intrusion Detection and Attack Classification using Back-propagation Neural Network". International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 3, March – 2014
[21] G. MeeraGandhi, "Machine Learning Approach for Attack Prediction and Classification using Supervised Learning Algorithms". International Journal of Computer Science & CommunicationVol. 1, No. 2, July-December 2010, pp. 247-250
[22] Jungles, P., Margosis, A., Simos, M., Robinson, L., & Grimes, R. "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques". June, 2013
[23] James Foster "Are there novel ways to mitigate credential theft attacks in Windows". SANS Institute, July, 2014
[24] Microsoft Corporation. "Cached and Stored Credentials Technical Overview". June, 2013
[25] Wang Jilong, Sun Mingmin, "Network Topology Discovery Based on IP Address Inferring". CHINA COMMUNICATIONS Volume: 9 Issue: 5, 2012, pp: 22-31
[26] Ingrid Bouwer Utne, Henrik Hassel and Jonas Johansson, "A Brief Overview of Some Methods and Approaches for Investigating Interdependencies in Critical Infrastructures", Risk and Interdependencies in Critical Infrastructures, Springer Series in Reliability Engineering 2012, pp1-11
[27] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science: Innovation for Humanity (SCEECS '12), March 2012.
[28] Mohammed A. Saleh, Azizah AbdulManaf, "A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks," Scientific World Journal, Hindawi Publishing Corporation, Article ID 238230, Volume 2015.
[29] Yigal Bejerano, Yuri Breitbart, Minos Garofalakis, Rajeev Rastogi "Physical Topology Discovery for Large Multi-Subnet Networks". IEEE INFOCOM 2003.
[30] Kwangjong Cho, Wonhyuk Lee, and Dongkyun Kim, "Self-Configurable Diagnosis Algorithm on an Isolation Network", Eighth International Conference on Networks, IEEE, 2009.
[31] H. Ray, R. Vemuri, and H. Kantubhukta, "Toward an automated attack model for red teams," IEEE Security and Privacy Magazine, Vol. 3, 2005, pp. 18-25.
[32] Graph Visualization Software, http://www.graphviz.org/.
[33] S. Zargar, J. Joshi, D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks", IEEE Commun. Communications Surveys & Tutorials, IEEE, Volume 15, Issue 4, 2013, pp. 2046 - 2069
[34] Tayebe Shokatpour, and Reza Ravanmehr, " A Survey on Discovery of Distributed Denial of Service Attacks in Cloud," International Journal of Computer Science Issues, Volume 12, Issue 3, May 2015
[35] "CLIPS: a tool for building expert systems," http://www.Clipsrules.sourceforge.net/onlineDocs.html

Adel E. Gomaa is Director General of Administrative and Engineering Affairs at the Ministry of Supply and Internal Trade, Egypt Received B.S. degree in computer science and engineering from Faculty of Electronics Engineering, Monoufia University, in 1992, He got the M.Sc. in Expert troubleshooting computer network system, EL-Azhar University ,2007.

Adly S. Tag El Dein is Professor (Associate) in Benha University, Dep. of Electrical Engineering (Faculty of Engineering at Shoubra), Egypt.
Received the B.S. Degree in Electronics and communication, Benha University in 1984 and the M.Sc. in computer based speed control of single phase induction motor using three level PWM with harmonic elimination, Benha University, in 1989. The Ph.D. in optimal robot path control, Benha University, in 1993. He is currently an Associate prof. in shoubra faculty of engineering and Manager of Benha university network and information center. And his research interests include Robotics, Networks, and Communication

Tarek El-Shishtawy is Professor of Information Systems at faculty of Computers and Informatics, Benha University Egypt, He got the Master and Ph.D. in Computer Engineering. As early as 1994, the author was interested in ICT4D, he built an expert system for poor farmers in Egypt. Now his research interests include intelligent systems for egovernments.Text Mining and Natural Language Processing.