Survivability-Oriented APT Penetration Analysis

Wang Pengfei, ZhaoWentao, Zhang Fan
School of Computer, National University of Defense Technology, Changsha, China
E-mail: wpengfei_nudt@163.com

***Abstract*— This article foremost introduces the survivability theory into the analysis of APT penetration, proposes the concept of penetration survivability and addresses it from the basic attributes of concealment, recoverability, self-adaptability and evolutionary. Proposed a survivability-oriented APT penetration analysis model -- PDMS, establishes the metric system by hierarchical analysis, constructs the knowledge base through statistical analysis, analyses and classifies the APT penetration through proper algorithm on the basis of the knowledge base. The feasibility is proved by actual APT penetration case analysis.**

Keywords - Penetration Analysis；Survivability；Advanced Persistent Threat;

I. INTRODUCTION

APT(Advanced Persistent Threat) is a kind of directed, complex network attack rise in recent years, usually launched by organizations (governments) or small groups, using a variety of advanced attack techniques and social engineering methods, penetrate into the target intranet step by step to obtain important assets and sensitive information[1]. Most of the targets of APT are business corporations, military organizations or governments, aimed at the destruction of industrial infrastructure, theft of important information related to national security, national economy and people's livelihood[2]. For example, In 2009, Operation "Aurora" against Google, resulting in the leakage of a large number of Gmail users sensitive information; In 2010, Stuxnet attack against Iran's nuclear facilities successfully drew the nuclear industrial level of Iran back to a few years ago, which was also the first attack case on industrial infrastructure in reality; In 2011, RSA SecurID theft attack making most company who use SecurID as the authentication credentials to establish a VPN network under attack, and important information get stolen.

The persistent penetration is the most significant feature of APT, which is also the key section during the implementation of APT. In order to hidden for several years without being discovered, APT penetration process has characteristics different from the general attack methods, for instance, it can avoid detection, conceal its trace, adapt to the complex environment, as well as evolution with knowledge learning, which can help it avoid the detection of defense system, making it a tenacious ability to survive. Analysis of the penetration process, and study of the penetration characteristics are of great significance to grasp the patterns of APT behavior, which is conducive to the detection and prevention of APT in the future. This article intends to introduce the concept of survivability into the research of APT penetration, and with the help of the attributes of survivability, we can do a comprehensive analysis on the penetrability of APT from concealment, recoverability, self-adaptability and evolutionary, which can contribute to revealing the APT intrinsic mechanism.

The article is organized as follows: Chapter 1 is an introduction; Chapter 2 related work, introduces the survivability theory and the existing problems of the traditional penetration analysis method, leads to the necessity of the use of survivability analysis of the penetration process; Chapter3 analyzes the APT penetration process and its characteristics, proposes a survivability – oriented model on APT penetration analysis; Chapter 4 verifies the feasibility of the proposed theory by the analysis of the actual APT case; and Chapter 5 is conclusion.

II. RELATED WORKS

Traditional permeation analysis methods focus on the multi-step behavior of penetration, usually combined with network topology, which gives an objective present of the penetration process, such as the penetration analysis model based on attack graph[3],and penetration test model based on petri net[4], but gives inadequate depiction of the characteristics of penetration. Especially with the rapid development of the complex means of network attack, like APT, the traditional analysis methods is demonstrated less effective when descript the new characteristics of concealment, recoverability and self-adaptability in penetration, which can hardly analyze penetration comprehensively.

The study of survivability starting in the field of war, aiming to minimize damage and save the lives of soldiers when the war equipment get damaged. In the late 1960s, the U.S. military standard formally defined it as the "ability of system to resist malicious environment when completing certain mission". The concept of information system survivability was firstly proposed by Neumann[5] from the U.S. Army Research Institute in 1993, defined as "Under any adverse conditions, the ability to continuously satisfying users' needs based on the application of computer communication system. " .CMU / SEI research team gave the most influential definition of survivability: The capabilities of system to timely complete its critical mission, when under attack, system failure or unexpected accidents [6].

Although research on survivability has been carried out for over ten years and it has a wide range of applications in the field of network systems, information systems, embedded systems, and hardware infrastructure, its

application mainly concentrate on the description of the system defense capabilities to recover from destruction, such as data confidentiality, integrity and availability, emphasis on "defense". Not yet anyone has introduced this concept to the analysis of network attacks, especially depiction of network penetration process, such as concealment, recoverability and self-adaptability of attack behavior, emphasis on "attack". With the help of multi-attribute characteristic of survivability theory, and combined with APT penetration characteristics, we can analysis comprehensively on the process of APT penetration, which will help to grasp APT behavioral features.

III. SURVIVABILITY-ORIENTED ANALYSIS ON APT PENETRATION

A. *Analysis on APT penetration*

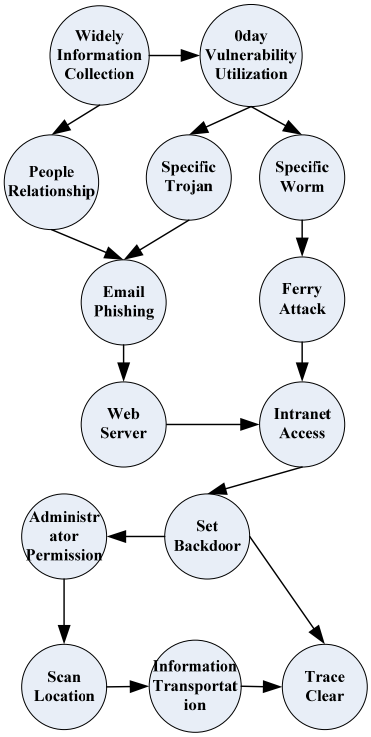

Figure1 General process of APT penetration

As shown in Figure 1, the general process of an APT penetration usually begins with widely information collection using some social engineering methods, afterwards, gain access to the internal network by taking advantage of the 0day vulnerabilities existing in the target system, then set backdoor, obtain authorization, and locate important information through continuously scanning the hosts within the internal network, finally transfer sensitive information through an encrypted tunnel and clear traces. The key technologies include email phishing combined with social engineering method, ferry attacks, SQL injection attacks, settings back door using Rootkit, gain permission using PI-RAT, information transportation using encrypted SSL tunnel.

As a kind of complex attack methods for targeted aims, APT has the characteristics like persistent and multi-step, utilizing a variety of advanced attack techniques and social engineering methods, to get access to the organization intranet step by step. Terms of purpose, hacker who launching an APT more often not for profit in a short time, but continuing penetration with the "springboard" of compromised host, establishing a large, controllable penetration network, until get a thorough handle of targeted information of certain things or people.

Although the traditional ways of penetration description, such as attack graph, is able to represent the process and state transformation of APT, it performs poor when depicting the complexity characteristics of APT, including its ability to avoid detection, ability to recover from destruction, ability to adapt to the complex environment, and ability of evolution through self-learning.

B. *Penetration Survivability*

Combine survivability theory with the characteristics of APT penetration process, and expand it on the basis of the original survivability attributes:

Definition 1: Penetration Survivability is the ability of network attack to successfully implement a penetration process, specifically including the ability to evade detection, the ability to recover from destruction, the ability to adapt to different system environments, and the ability of evolution after knowledge learning.

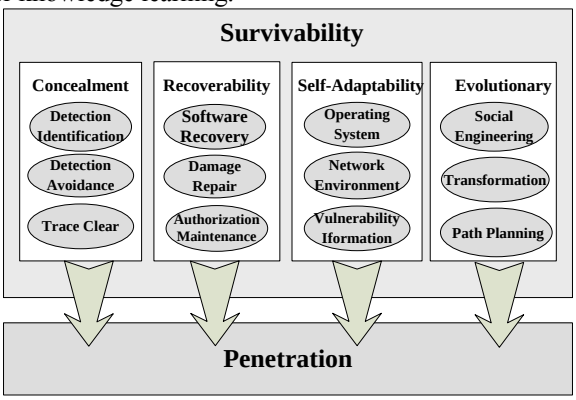

Figure 2 Illustration of Penetration Survivability

Then we propose a penetration descriptive model based on the concept of penetration survivability:

Definition 2: Penetration Descriptive Model based on Survivability, PDMS = {C, R, A, E}, where:

Concealment set， representing the ability to evade detected by system defense facilities during penetration process, including detection identification, detection avoidance, trace clear , denoted by C.

Recoverability set, representing the ability to recover from destruction, failure, or unexpected accident when discovered by network system defense facilities, including the ability of anti-virus software recovery, damage repair, and authorization maintenance, denoted by R.

Self-adaptability set, representing the adaptive capability to the target environment, including operating system,

network environment and the vulnerability information, denoted by A.

Evolutionary set, representing the evolutionary capability generated after learning knowledge and environment information, including utilization of social engineering method, transformation, and capability of penetration path, denoted by E.

C. Penetration Descriptive Model based on Survivability

Step 1：Metric extraction of penetration

Establish the metric system by hierarchical analysis of the APT penetration with Analytical Hierarchy Process, and abstract the target layer, penetration layer as well as atomic layer, as shown in Figure 3.

The penetration layer is constructed by the key steps in APT penetration process, including information collection, vulnerability utilization, intranet access, horizontal expansion, and assets transportation. The atomic layer represents the key techniques used in each penetration step.

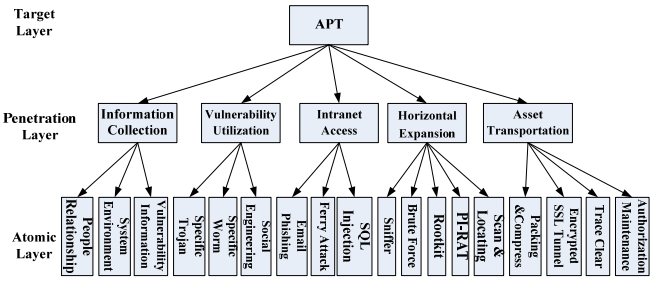

Figure3 APT hierarchical analysis

Step2：Construction of Knowledge Base

Choose five most famous penetration case of APT[7] for statistical analysis, as is shown in Table 1, determine the metric weights of the atomic metrics extracted in step1 according to the usage frequency of each technique, to build the knowledge base.

Definition 3：Knowledge Base, is a set of 2-tuple, $KB=\{(a_i,w_i)\}$, i=1,2,…n, n is the total number of the related atomic metrics. Where a_i represents the atomic metrics of the metric system， w_i represents the corresponding atomic metric weight, which is determined by statistical analysis.

Table1 Knowledge Base

Penetration Layer	Atomic Layer Metrics	2009-2010 Operation Aurora	2007-2011 Operation Night Dragon	2011 RSA SecurID Attack	2010 Stuxnet Attack	2006-2011 Operation Shady RAT	Score Weight (%)
Information Collection	People Relationship	√	√	√	√	√	100
	System Environment	√	√	√	√	√	100
	Vulnerability Information	√	√	√	√	√	100
Vulnerability Utilization	Specific Trojan	√		√		√	60
	Specific Worm				√		20
	Social Engineering	√	√	√		√	80
Intranet Access	Email Phishing	√	√	√		√	80
	Ferry Attack				√		20
	SQL Injection		√				20
Horizontal Expansion	Sniffer	√					20
	Rootkit	√	√	√	√	√	100
	Brute Force		√				20
	PI-RAT		√		√		40
	Scan &Locating	√	√	√			60
Asset Transportation	Packing &Compress	√	√	√			60
	SSL Tunnel	√	√	√			60
	Authorization Maintenance		√		√	√	60
	Trace Clear			√	√		40

Step3：Attribution of survivability

Choose the proper penetration survivability attributes for each atomic metric generated in step 1 as shown in Table 2.

Table2 selection of survivability attributes

Penetration Survivability				
Atomic Layer	***C***	***R***	***A***	***E***
People Relationship			√	√
System Environment	√	√	√	√
Vulnerability Information			√	√
Specific Trojan	√		√	
Specific Worm		√	√	
Social Engineering	√			√
Email Phishing	√			
Ferry Attack			√	
SQL Injection	√			
Sniffer	√		√	
Rootkit	√			
Brute Force			√	
PI-RAT		√		
Scan &Locating		√		√
Packing &Compress	√		√	
SSL Tunnel	√		√	
Authorization Maintenance		√		√
Trace Clear	√			√

Step4：Calculation of survivability attributes

Calculate the score of each survivability attribute, according to knowledge base (Table 1) and attributes selection(Table 2), algorithm is shown in Algorithm 1.

Algorithm1 Calculation of attributes

Input: $A=\{a_i\}$, $i=1,2,\ldots,n$
Output: $S=\{S_C,S_R,S_A,S_E\}$
While $X \in \{C,R,A,E\}$
  for i from 1 to n
    if $relatedAttribute(a_i, X)$ then
      $S_X=S_X+w_i$

Step5：Result Classify

Analyze and classify the score of the calculation result according to Table 3.

Table3 Standard of Classify

No.	Range	Level	Description
1	S≥600	Very Good	Outstanding performance in that attribute.
2	400≤S＜600	Good	Performs well to present that attribute.
3	200≤S＜400	Middle	Basically performs that attribute.
4	S＜200	Bad	Performs bad in that attribute.

IV. CASE VERIFICATION

Select the RSA SecurID theft attack as a penetration scenario for analysis, to prove the feasibility of our proposed model.

Firstly, determine the atomic metrics of the penetration scenario, as shown in Table 4.Then calculate with knowledge base shown in Table 2, to get the scores of concealment, recoverability, self-adaptability and evolutionary are as follows:

S_C=100+60+80+80+100+60+60+40=580.
S_R=100+60=160.
S_A=100+100+60+60+60=380.
S_E=100+100+60+40=300.

Table 4 RSA SecurID Theft Analysis

Penetration Layer	Atomic Layer	RSA SecurID Attack	Weight (%)
Information Collection	People Relationship	√	100
	System Environment	√	100
	Vulnerability Information	√	100
Vulnerability Utilization	Specific Trojan	√	60
	Social Engineering	√	80
Intranet Access	Email Phishing	√	80
Horizontal Expansion	Rootkit	√	100
	Scan &Locating	√	60
Asset Transportation	Packing &Compress	√	60
	SSL Tunnel	√	60
	Trace Clear	√	40

Finally classify the result according to Table 4. To draw a conclusion, the penetration process of the famous RSA SecurID theft attack, performs well in concealment, basically have the ability of self-adaptability and evolutionary, but performs bad in terms of recoverability.

V. CONCLUSION

The contribution of our work can be submitted as follows: introduced survivability theory into the analysis of APT penetration and proposed the concept of penetration survivability, proposed a survivability-oriented penetration analysis model -- PDMS model, to comprehensively analysis an APT penetration process from concealment, recoverability, self-adaptability and evolutionary, and classify the analysis result. Real APT penetration scenario analysis with PDMS verified the feasibility of the proposed model. The following work concentrate on enriching the knowledge base, and optimizing the quantization algorithm to improve analysis accuracy.

REFERENCES

[1] Huang Dali, Xue Zhi. Research and Analysis on Advanced Persistent Threat Behavior[J]. Information Security and Communication Secrecy, 2012, 5.

[2] Bo Na. APT : Hiden , Aims at Theft of Enterprise Secret [J]. Journal of China Computer, 2012.

[3] Cui Ying, Zhang Lijuan, Wu Hao. Automatic generation method for enetration test programs based on attack graph[J]. Journal of Computer Applications, 2010, 30(8).

[4] Yang Tao, Guo Yixi, Zhang Hong. Application of Colored Petri Net in Penetration Test[J]. Computer Engineering, 2009, 35(1).

[5] Hollwya B A, Neumann P G. Survivable Computer-communication Systems: The Problem Working Group Recommendations[R]. Technical report AL-CE-TR-92-22, Washington: Army Research Laboratory, 1993.

[6] Fisher J, Linger R. Survivability: protecting your critical systems[J]. IEEE Journal of Internet Computing, 1999, 3(6): 55~63.

[7] Huang Xin. Share of APT Attack Case[EB/OL]. http://wenku.baidu.com/view/497134d2b14e852.