機械学習を用いたネットワーク走査活動の分類

ゴ　キム　クォン†　　中村　康弘†

†防衛大学校
239-8686 神奈川県横須賀市走水 1-10-20
em53039@nda.ac.jp, yas@nda.ac.jp

あらまし 一般に，サイバー攻撃における攻撃者は，その攻撃活動あるいはマルウェア拡散を目的として，脆弱性を持つホストやサービスを探すネットワークスキャンを実施する．スキャン活動の監視と分析は，組織 LAN を外部からの不正な攻撃から守るための侵入検知や侵入防止等の対策において，重要な役割りを担う．また，マルウェアの拡散を低減，停止することができる．この研究の目的は，ネットワーク走査活動の兆候を発見し，分類するために，ネットワークトラフィックを分析することである．複数のネットワークトラフィックの特性を調査し，観測された走査パターンをいくつかの走査活動に分類する．走査活動の種類を判別するために機械学習を用いる．

Network scanning activities classification using machine learning

Ngo Kim Cuong†　　Yasuhiro Nakamura†

†National Defense Academy
1-10-20, Hashirimizu, Yokosuka, Kanagawa 239-8686, JAPAN
em53039@nda.ac.jp, yas@nda.ac.jp

Abstract Usually, cyber attackers perform network scanning to look for certain services or hosts with certain vulnerabilities to attack or spreading malwares. Monitoring and analyzing scanning-activity play an important role in network intrusion detection and prevention, both to protect individual networks against malicious outside attacks. It may also mitigate or stop global outbreaks of malwares. This research target is to analyse network traffic for discovering and classifying properties of network scanning activities. Several characteristics of network traffic are investigated, and the observed scanning patterns are classified to some scanning activities. Machine learning is applied to classify the type of scanning activities.

1 Introduction

Network scanning is a favourite approach of cyber attackers. It's one of the first steps to gather information about the target computing systems and networks. Essentially, network scanning consists of network port scanning as well as vulnerability scanning. Network port scanning send messages to specified service port of the target system. The kind of responses indicates whether the port is used and can therefore be probed for weakness. Vulnerability scanning is a method used to discover known vulnerabilities of computing systems that available on a network. It detects specific weak spots in an application software or the operating system, which could be used to determine whether computer systems are vulnerable to attack or spreading malwares. The important element of security is understanding the attackers, to learn about their techniques, tactics, intentions, and motivations. A Honeynet usually have been deployed, because the Honeypot serve as one potential source of malicious data.

Honeypot is a decoy system designed for the

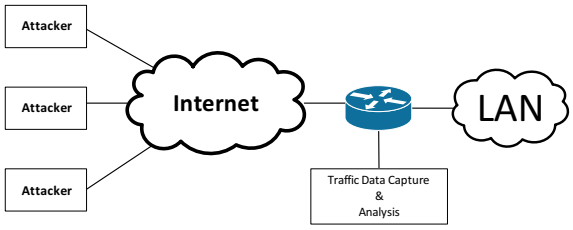

Figure 1: Observation of attack activities

purpose of diverting an attacker from accessing critical systems and capturing samples of malwares infections so that their behavior can be analyzed in detail. It also helps to identify their preferred attack targets and methods, shown in Figure 1. However, Honeypot produces a lot of data that make it difficult to analyze.

In this paper, simple responder like a low interaction Honeypot is used to collect data. This responder communicate back to the connection request from an attacker, then the Honeynet collected all the information about initial connection, its respond and initial payloads. After that the behavior of the connection request and its initial payloads can be classified into the type of the attack. Based on these classification result, these collected data will be recognized that how many attack types were detected. To classify them, machine learning methods are utilized, it is also known as data mining algorithms.

Classifying and identifying scanning activities will help the network administrator to recognize and analyze these methods of attacks.

2 Related Work

There were many research papers proposing some different methods and various classification algorithms to detect and to classify network scanning activities. Vahid Golmah[1] proposed a hybrid intelligent system uses the approach of integrating different learning or decision making models. Each learning model works in a different manner and exploits different set of features. He thought his integrating different learning models gives better performance than the individual learning or decision-making models. But actually the overall functioning of the system depends on the correct functionality of all the layers. Bhavna Dharamkar[2] proposed a improved ensemble method, based on Neural Networks and Gaussian Support Vector Machines, for cyber attack classification. Experiments with the KDD Cup 1999 dataset[4] show that SVM-NN can provide, the better generalization ability and effectively classified cyber attack data. Abedelaziz Mohaisen and Omar Alrawi[3] used different machine learning algorithms on classifying Zeus which is a popular malware family. These works are classified based on behavior detection approach and they generated the dataset themselves.

Most of them used KDD Cup '99 dataset in their experiments, but it is over 15 years old and out of date for newer malwares, it's no longer reflect realistic attacks.

For classification of scanning attacks, effective features will be selected and used to machine learning. Especially, detection of unknown activities is as important as detection of known activities for network management. Then, in this paper,a typical activity model will be generated from previous captured packets, detection and classification of attackers behavior to estimate attackers intentions.

3 Machine Learning

3.1 Algorithms

Machine learning is a sub-field of Artificial Intelligent, and it is making most of the progress in Artificial Intelligence today. Machine learning system can learn training patterns to recognize and classify new unknown patterns. There are many algorithms for classification. In this research, Decision Tree C4.5 is adopted because it can be applied to real-time detection system in future.

3.2 Feature Selection

Usually, darknet observation system is using almost all of IP header fields for analyzing them. Another method such as sFlow based on attributes of a TCP flow, min/ave/max packet

sizes, flow duration time, etc. But this research targets to observe the first payload from attacker, which may includes darknet scanning activities, malwares infection activities, and so on. First of all, the payload arrival activities are investigated, then the following several facts are revealed.

- This simple responder can get only first payload for each connection request.
- For each darknet addresses can be received many payloads for any time.
- The same source address usually sends the same payloads, continuously.
- Sometime, the same payloads are received from many different source addresses.

From these above conditions, some features are selected for each source IP address as shown in table 1. The pre-observation results are indicated in Table 2. Each range of values is regarded as a class.

4 Proposed Method

4.1 Model construction

To classify each attack payloads that arrived to darknet, a model is constructed using some features shown in table 1. Six kinds of features each has three or four ranges, then all number of model is 4*3*3*4*4*3 = 1,728 classes. Typical values are prepared and combined and generated model data is used as a training data for machine learning algorithm. This training dataset will be used for model learning.

4.2 Network Observation

Network interface of organization LAN to Internet is mirrored to a packet capture device. Captured packet and which header values and payloads are investigated for classification. This observation and analysis procedure will be repeated every N minutes. All of the arrival packet while each N minutes, will be classified to above model classes. Usually, packets which came from the same IP address has the same characteristics and is classified to same class. But, if the feature has changed from the middle of iteration, it is discriminated to the another class.

Table 3: Classification results

Number of classified class	Number of IP address
1	4,831
2	1,152
3	633
4	210
5	67
6	28
7	30
8	11
9	6
11	1
13	1
19	1

4.3 Classification

Observed features are used to classify and to investigate that each packets can be classified to known classes or not. Especially, packet which has low prediction error rate will be found, it must be concerned for capability of new attack pattern or attacker change the tools.

4.4 Experimental results

Extracted features from all packets for every 10 minutes are classified pre-builded classes shown in Table 3. 4,831 of them indicated only one class, but the others belongs 2–19 classes. It may be estimated to the fact that attacker changes the attack tool, initial or terminate the attack scheme, or some environment has been changed. It is needed collect more detail in investigation of the change of packet behaviors.

5 Conclusion

Model based packet classification method is proposed for packet observation by simple Honeypot. From the last observations, 1,728 basic classes are constructed and trained. And, packets which arrived every 10 minutes from

Table 1: Observed features by simple Honeypot

name	description
`dstip`	Number of destination IP address.
`sport`	Number of source port numbers.
`dport`	Number of destination port numbers.
`hash`	Fuzzy hash value of payload.
`span`	Average time for each arrival time of payloads.
`sdev`	Standard deviation of above `span`.

Table 2: Observed feature values

Num	Name	range	class No.
1	dstip	1, 2-9, 10-99, 100-	1,2,3,4
2	sport	1, 2-99, 100-	1,2,3
3	dport	1, 2-99, 100-	1,2,3
4	hash	1, 2-9, 10-99, 100-	1,2,3,4
5	span	<0.1, 0.1-0.9, 1.0-10.0, 10.0<	1,2,3,4
6	sdev	<1, 1-10, 10<	1,2,3

Internet has been captured and extract features and payloads. Finally, each packet will be classified to one of model class.

Experimental results shows that packets from same IP address are not always same attack pattern. It is estimated that attacker change the attack software, start new attack scheme or change some environment of network. That must be concerned for detection or prevention new attacks.

References

[1] V. Golmah, "An Efficient Hybrid Intrusion Detection System based on C5.0 and SVM", Int. J. of Database Theory and Application, Vol.7, No.2, pp.59–70, 2014.

[2] B. Dharamkar, R. R. Singh, Cyber-Attack Classification using Improved Ensemble Technique based on Support Vector Machine and Neural Network Int. J. of Computer Applications, Vol.103, No.11, Oct. 2014.

[3] A. Mohaisen, O. Alrawi, Unveiling Zeus: Automated Classification of Malware Samples, WWW '13 Companion Proceedings of the 22nd International Conference on World Wide Web, pp.829-832, 2013.

[4] The UCI KDD Archive, KDD Cup 1999 Data, Information and Computer Science, University of California `http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`

[5] Weka 3.7.0 tools [Online], `http://www.cs.waikato.ac.nz/ml/weka/` (July 2, 2009)