Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 155 – 165

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Neural Network Based Approach for Stepping Stone Detection under Delay and Chaff Perturbations

Rahul Kumar, B.B.Gupta*

National Institute of Technology Kurukshetra, India

**gupta.brij@gmail.com*

Abstract

The way attackers execute attacks is incredible, they execute attacking commands form intermediate compromised host to remain anonymous instead from their own computers. These intermediate hosts are called as stepping stone host and attacks that attackers perform using stepping stones are called as stepping stone attacks. One solution to the problem of stepping stone attack is to detect stepping stone host so that we can break attacking path created and used by the attacker. In this paper, we propose a stepping stone detection approach which analyses the traffic flowing through the host to find out whether this is a stepping stone host or normal host. Our approach classifies traffic into two categories Stepping Stone Traffic and Normal Traffic using Neural Network. If the traffic flowing through the host belongs to the class of stepping Stone Traffic this indicates that host whose traffic is being tested is a stepping stone host otherwise it is a normal host. Our approach allows attacker to insert chaff packets and fixed delay, reshuffling of packet, padding, and encryption of attacking traffic.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Neural Network, Stepping Stone Host, Packet Context, Stepping Stone Traffic

1. Introduction

There is tremendous change in the way computers can be used since the concept of Internet and Networks has arrived. The way Internet has revolutionized the use of computers in business, education and various other fields is quite appreciable. Enhancement and development of new technology has increased application of Internet and its efficiency [23].But true fact is that nothing can be perfect in all dimensions; the same concept is also applied on the Internet Technology. Although Internet has wide range of application in different fields and also provides large number of benefits to humans, but it also has got some weaknesses as well which are known as web application vulnerabilities [25-28]. Cybercriminals also known as attacker exploits these vulnerabilities to execute cyber-attacks

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.204

against computers and application connected to Internet [21-22, 29-32]. As we have mentioned above that the enhancement, development of new tool and technologies has increased applications of Internet. These tool and technologies add number of vulnerabilities to Internet Technology. The type of attack is defined by the type of vulnerability being exploited by the attacker; there are different kind of vulnerabilities such as software vulnerabilities, hardware vulnerabilities and many more.

As the number of vulnerabilities are increasing the number of attacks is also increasing, attackers are developing and executing new attacks by exploiting these vulnerabilities [22]. There is a wide range of attacks that attackers can execute such as malware attacks, phishing attacks DoS attacks and the list is endless [24]. Attacker always remain one step ahead of the security professional and search for holes in the security system, and then exploit them to execute attack. Attackers always look for safe path that they can follow to remain anonymous while executing attacks. In order to remain anonymous they use anonymity techniques such proxy, which was develop with an aim to surf Internet without revealing identity to other users. But nowadays attackers use proxy while executing attacks [20]. Another technique that attacker use to remain anonymous is to use stepping stones in the path while execute attacks. The attacks that attacker perform using stepping stone are called stepping stone attacks. Stepping stone are intermediate host that attacker compromised to use them while executing attacking command [1, 2]. In stepping stone attack, attackers use scanning techniques to find out computers having low quality security management and then compromise it to take full control over it. After that attacker use previously compromised computer system to compromise other and also take control of newly compromised system and so on, in this way attacker form a chain of connection through intermediate compromised host. Such a chain of connection is known as stepping stone connection chain and intermediate host that exist on connection chain is known as stepping stone host, any pair of connection in the chain is known as stepping stone connection pair. Finally the attacker executes attacking command from the last stepping stone host in the chain [1, 2, 3, 4]. Stepping stone attacks are more dangerous as compare to other attacks because they are quite flexible and can be used to perform any kind of attacks such malware attack, phishing attack, DoS and DDoS attacks and many more, which make them a major threat for computer and data security [9].

One possible solution to the problem of stepping stone attack is to detect stepping stone that has been created and used by the attacker, once we have found stepping stones we can filter and block the malicious traffic flowing through it. Many stepping stone detection techniques have been proposed by the researchers to prevent and detect stepping stone attacks. Most of them are vulnerable to some evasion technique. This motivated us to propose new stepping stone detection technique non-vulnerable evasion techniques. Proposed technique is based on two previously existing approaches, the *Neural Network Approach* given by *Wu and Huang* [6] and *Packet Context Approach* given by *Jianhua yang and David woolbright* [15]. In [6] Wu and Huang have mentioned that neural networks have the ability to analyse and classify network activity, by using this idea we differentiate between the normal traffic and stepping stone attacking traffic. In our proposed approach we also use the concept of *packet context* given by *yang* and *woolbright* in [15]. The packet context approach given in [15] correlate incoming and outgoing connection using the concept of *packet context*, on a host to identify whether it is a stepping stone host or normal host. Problem with this approach is that it cannot work well if host for which we are testing have only few incoming and outgoing connection. Thus in order to overcome the limitations of *packet context* approach we combine *Neural Network Approach* with *Packet Context Approach*. Advantages of packet context approach is that it is not vulnerable to chaff and delay perturbation and also have high detection rate thus our proposed scheme by default inherit its qualities and also work well even if a host have only few incoming and outgoing connections. Rest of the paper is organized as follows, in section 2 we discuss related work. In section 3 we define our proposed approach for stepping stone detection and in section 4 we discuss results implementation details. In section 5 we conclude this paper.

2. Related Work

Many detection techniques have already been proposed in recent decade for stepping stone detection. First detection approach was developed by Staniford-Chen and Heberlein [1] this approach was based on the packet's