Preface

Vulnerability Analysis is a process that defines, identifies, and classifies the vulnerabilities in a computer network or an application. Vulnerability in a network or application can in turn be used to launch various attacks like cross-site scripting attacks, SQL injection attacks, format string attacks, buffer overflows, DNS amplification attacks etc.

Although these attacks are not new and are well known, the number of vulnerabilities disclosed to the public jumped nearly 5 percent during the first six months of 2007. This accounts to be the fourth year report, which shows the raise in vulnerability (see the news link on security focus http://www.securityfocus.com/brief/614). In January 2007, a vulnerable network resulted in a theft of 45.6 million credit card numbers in TJX companies due to unauthorized intrusion.

A good protocol analysis and effective signature writing is one of the effective method to prevent vulnerability and minimize the chances of intrusion in the network. However, protocol analysis poses two challenges namely false positive and evasion. If the signature to prevent the vulnerability is not written properly, it will result in dropping of a valid traffic thereby resulting in false positive. An effective signature should also consider the chances of evasion; otherwise a malicious attacker can use the variant of exploit and evade the protection provided by the IDS/IPS.

This book discusses the structure of protocol and provides a thorough understanding of the structure, which is crucial in writing signatures. It also discusses the pseudo code of algorithms, which can be used to reduce false positives. The chapters in this book are prepared with an assumption that the reader is familiar with the protocols and RFC of various protocols. The reader should also have knowledge on using basic tools like ethereal.

Chapter 1 deals with wireless networks. This chapter elaborates the flaws in Wireless networks, and also confers about the tools, which can be used to find out whether the current deployment of wireless network is vulnerable for an attack. Due to the complexity of preventive measures, the TKIP and AES- CCMP are discussed in-depth.

In Chapter 2, the Mail Protocol and the vulnerabilities associated with the POP, IMAP and SMTP are explained. Format string vulnerability and the buffer overflow attacks are discussed in detail in this chapter. Vulnerability analysis requires checking the arguments of commands for malicious patterns. In case of SMTP traffic, the signatures will be checking for the SMTP commands as well as the

data in it. If the signatures are active in the data part of SMTP traffic, then it will result in dropping of a valid email thereby, resulting in a false positive. A case study of false positive in SMTP and IMAP traffic along with the algorithm to prevent the false positive is elaborated.

In Chapter 3, the FTP and TFTP protocol are explained. FTP protocol is prone to direct traversal attacks and buffer overflow attacks. The methods, which can be used to prevent these attacks, are also discussed. Structure of TFTP protocol with the opcodes and methods used to remove MS DOS device name attack, buffer overflow attack are also explained.

Chapter 4 deals with HTTP. Cross-site scripting attack, SQL injection attack and MS DOS Device name vulnerability are the most important attacks in HTTP. The intricacies of these attacks and the preventive measures of the attacks are discussed. Due to various encodings in HTTP, signatures are prone to evasion. As Oracle is the most commonly used database server, this chapter discusses the TNS protocol structure in detail. Methods to reduce false positive is represented with the help of flowchart and algorithm.

Chapter 5 deals with the structure of DNS /DHCP protocol and the algorithm. The algorithm ensures that the signatures (to prevent vulnerability in the protocol) are active only in the desired part of DNS/DHCP traffic. The algorithms aid in minimizing false positives. The chapter also details about the various attacks like DNS cache poisoning, DNS amplification attack and DNS hijacking attack.

Chapter 6 discusses the details of LDAP, SNMP and the ASN BER encoding. LDAP and SNMP protocol uses ASN, BER encoding. Understanding of ASN and BER syntax is required to identify the commands in LDAP and SNMP.

Chapter 7 focuses on the RPC protocol and the NDR encoding. The pseudo code of the algorithm, which ensures that the vulnerability specific rules are sanitized (only on specific parts of the RPC traffic) are discussed. The chapter discusses the Algorithm for both RPC over SMB and RPC over TCP. RPC traffic is prone to various evasions. The Port mapper in RPC is also elaborated.

Chapter 8 deals with malware. The chapter starts with the naming convention, which can be used for naming the malware. It then discusses about the confinement using hard virtual machines, soft virtual machines, jails, chroot, sensors and system call spoofing. The chapter then discusses about the rootkits, and preventive measures. The spyware and the preventive measures of Spyware are also discussed.

Chapter 9 focusses on reverse engineering. The chapter deals with linear sweep disassembler, recursive traversal disassembler and various evasion techniques, which can be used by disassembler. The detection of hardware break point, software break point and, detection of virtual machines are also presented. The chapter is concluded with the methods that are used to find the manual entry point of an executable and import table reconstruction.

The concepts that are discussed in this book is practical and will inculcate interest to the reader. To ensure a better understanding, the packet captures are taken from the real world exploits and the algorithms are presented in the form of flow charts. These algorithms can be converted into any language.

Although, the book has been designed for those who practice information security, the book can also be used for advance level network security courses. The instructors can feel free to contact.

Abhishek Singh

http://www.springer.com/978-0-387-74389-9

Vulnerability Analysis and Defense for the Internet
Singh, A. (Ed.)
2008, XVI, 254 p., Hardcover
ISBN: 978-0-387-74389-9