Abstract

Computer networks are certainly vulnerable as long as they deliver services from different machines. An attack graph is a security model representing the chains of vulnerability exploits in a network displays the ways an attacker can compromise a network or host. A number of researchers have admitted attack graph visual complications and a large amount of source data must be assembled to accurately build an attack graph, the difficulty scaling to large, enterprise-size networks with tens of thousands of hosts and the lack comprehensive understanding. Information on vulnerabilities is present in public vulnerability databases, such as the National Vulnerability Database and Nessus. But current attack graph tools are reserved to only limited attributes. The automatic formation of vulnerability information has been troublesome and vulnerability descriptions were created by hand or based on limited information. Much vulnerability has still not been discov-ered and many others without patches or solutions Our approach to developing a cost metric exploits the Markov’s model using combinations well known vulnerabilities (the Common Vulnerability Scoring System, CVSS) and Risk Assessment Values (RAV) and using ranking algorithms (similar to V. Mehta et al. 2006
and kijsanayothin, 2010) but instead of using vulnerabilities. For each host we have developed
a cost rank Markov’s model reducing the complexity in the attack graph, representing the
network topology and dipping the problem of visibility.

Reference

  Springer-Verlag.
  SANS Institute, June 2007.
  Secunia Half Year Report 2010,
  graphs. In D. Zamboni and C. Kr “ugel (Eds.), Recent Ad- vances in Intrusion Detection, Volume
  4219 of Lecture Notes in Computer Science, pp. 127–144. Springer.
- Phongphun Kijsanayothin, Network Security Modeling with Intelligent and Complexity
  Analysis, 2010.
- ISEGCOM, SCARE 0.1 - The Source Code Analy-sis Risk Evaluation 15. November
  IEEE Computer Society.
  10-July-2008.
- S. Noel, M. Jacobs, P. Kalapa, and S. Jajodia. Multiple Coordinated Views for Network
  Attack Graphs. In VIZSEC’05: Proc. of the IEEE Work-shops on Visualization for Computer
- S. Noel and S. Jajodia. Understanding Complex Network Attack Graphs through
  Clustered Ad-jacency Matrices. In ACSAC ’05: Proceedings of the 21st Annual Computer
  Computer Society.
  Re-search and Development Canada, September 2007.
  Netw. ISDN Syst. 30(1-7), 107–117.

**Index Terms**

Computer Science  
Security

**Key words**

Network security  
Security metrics  
Ranking attack graph