Honey-patterns: Recognizing Pattern based Attacks on Websites

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 161
Number 9

Year of Publication: 2017

Authors:
Prathamesh P. Churi, Shreya Bondre, Neha Gavankar

10.5120/ijca2017913202

Abstract

The exact definition of a honeypot is contentious. However, the concept can be defined as “A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server functioning normally, but all the data and transactions are phony. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine the vulnerabilities of the system” Honeypot is a closely monitored decoy that is employed in networks to study the trail of hackers and to alert network administrators of a possible intrusion. Honey net is a method for detection of abnormal activity in the network. Honey net is an additional layer of security. Even though it is not a panacea for security breaches, it is useful as a tool for network forensics and intrusion detection. Data Capture and Data Control are properties of honeyed, used extensively by the research community to study issues in network security, such as Internet worms, Spam control, DoS attacks, etc. In this paper, we will be focusing on the attack part.

References
3. Sams. Teach Yourself My-SQL in 21 Days
4. Software Engineering by TATA mc-graw hill publications
5. Learning PHP and MySQL by O’REILLY publications

Index Terms

Computer Science
Security

Keywords

Security, tools, installation problem, framework, designing, projects, Web application