|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clientes | Métodos e Procedimentos | Objetivo | Justificativa | Referencial bibliográfico |
|  |  |  | Os ataques do tipo *zero-day*, são imprevisíveis. Isso devido porque essas falhas que permitem os ataques elas não foram divulgadas publicamente, e com isso o *software* não pode ser corrigido e os antivírus não conseguem detectar o ataque através da assinatura baseada em assinatura. | BILGE, LEYLA; DUMITRAS, TUDOR. Before we knew it: an empirical study of zero-day attacks in the real world;  EGELMAN, SERGE; HERLEY, CORMAC; C. V. OORSCHOT, PAUL. Markets for Zero-Day Exploits: Ethics and Implications;  FOTI, PAOLO; ARMIN, JART; CREMONINI, MARCO. 0-Day Vulnerabilities and Cybercrime;  KUMAR, PRATAP; K. SETH, RAVI. A Review on 0-day Vulnerability Testing in Web Application;  LAST, DAVI; Forecasting Zero-Day Vulnerabilities;  LUO, TIANYNUE; NI, CHEN; HAN, QING; YANG, MUTIAN; WU, JINGZHENG; WU, YANJUN. POSTER: PatchGen: Towards Automated Patch Detection and Generation for 1-Day Vulnerabilities. |
| Recursos necessários | Capítulos e seções |
|  |  |