Intrusion Detection on Campus Network, the Open source approach: Accra Technical University Case Study

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

Volume 164
- Number 6

Year of Publication: 2017

Authors:
Victor Gbedawo, Komi Agbesi, Theophilus Adukpo

10.5120/ijca2017913664

Abstract

The computer network security landscape in recent times has become a crucial area in computer networking for both network administrators and network users such that, a compromise of this network security makes the services it provides and more importantly the data it holds, highly susceptible to exploits by malicious people for different purposes and reasons. This is particularly so for campus networks in view of the fact that, they do not only provide services to promote academic work directly but in many ways are integrated into the administrative setup of the institutions they serve. This research therefore seeks to investigate the security threats and vulnerabilities of campus networks and systems to a great extent, so as to propose interventions to resolving these threats, vulnerabilities and exploits, so as to improve the security of these networks by conducting a penetration test that simulates Intrusion Detection employing free and open source software (FOSS) tools. The research adopted “Cloppert’s kill chain” Approach to Penetration Testing. The elements of the simulation included the following FOSS tools VMware Fusion (Operating System simulator), Zentyal Server (unified network server), Snort (Intrusion Detection System), Suricata (Intrusion Prevention System),
Intrusion Detection on Campus Network, the Open source approach: Accra Technical University Case Study

Nmap (Network scanning), OpenVAS (Vulnerability Assessment Software) and Metasploit Framework (Exploitation tool). Results of the simulation revealed injection flaws to be the prevalent security vulnerability that was exploited and hence, discussed to improve computer network and application security in a rather cost effective fashion.

References


Index Terms

Computer Science
Information Sciences

Keywords

OWASP top 10, ‘Kill Chain approach’, Zentyal server, IDS/IPS, OpenVAS, NVT feed, CVE, SQL injection, Denial-of-service attack, Overt and Covert attacks