

Security Penetration Testing with VMWare and Kali Linux in a Wired Environment

R. S. Craven Email: rcraven.063089@student.uwtsd.ac.uk

School of Applied Computing, University of Wales Trinity St David, Mount Pleasant, Swansea, SA1 6ED,

Introduction:

Virtualization software, VMWare Player, will be used to create a network of five systems; four networked with three running Windows 7, one running Windows Server 2008 and a fifth system running Kali Linux. Once the four Windows-based systems are operating, the Kali Linux system will be used to demonstrate the vulnerabilities of a network with various degrees of security.

Aims & Objectives:

The aim of the project is to review network security from 2 sides:
The Network Administrator, building the network and installing all the security features as advised by the National Institute of Standards and Technology's Computer Division [3] and
The Hacker, using Kali Linux and the various pieces of software it features to attempt to access or disable the network.

Ref:

[1] T. Bittman, P. Dawson, M. Warrilow, <https://www.gartner.com/doc/reprints?ct=160707&id=1-3BgFAMo&st=sb>, Gartner, 2016

[2] D. Dieterle, Basic Security Testing with Kali Linux, Marston Gate, 2014

[3] P. O'Reilly, L. Feldman, G. Witte, Computer Security Division Annual Report 2015, NIST, 2016



Attacks & Software [2] :

- Metasploit - take control of the target machine and access programs to spy on the target.
- Recon-NG – to perform information gathering and network reconnaissance.
- Arpspoof – perform Man in the Middle attacks to intercept network packets.

Why VMWare Player:

VMWare Player has been chosen as the virtualization software to be used in this instance for a number of reasons:

- According to the Gartner Report [1] it is one of the market leaders for functionality and scalability.
- VMWare is one of the least used virtualisation softwares for creating an environment for academic testing purposes.

Research:

The research methods strategies for this project :

- Experimental with manipulation of the security and attacks
- Case Study with the data collected.

