

Prevention Detection and Hacking

Jordan Luxton P139822

Introduction

Prevention, detection and hacking will demonstrate the effective uses of open source software[1] which is free and community driven. The project is being developed with an emphasis on managing, emulating and protecting enterprise business networks, whilst also demonstrating penetrations testing. The project is derived from all 2016 high scale networks attacks with 2/3rds of business in the UK being effected by such attacks [2].

Aim's

To demonstrate effective and freely available hacking software whilst combating it with strong security community driven software. From that software, the development of two networks system using both wired and wireless scenarios demonstrating fundamental differences in abilities to protect networks.

Methods



Figure .1 GNS3 VMware software

The project environments are being developed in both simulation and real world. Through the tools such as GNS3[3] and vmware[4] the large enterprise networks will be placed and attacked with one network being poorly configured with minimal protection and the other network being the gold standard having high security policies.

Hacking

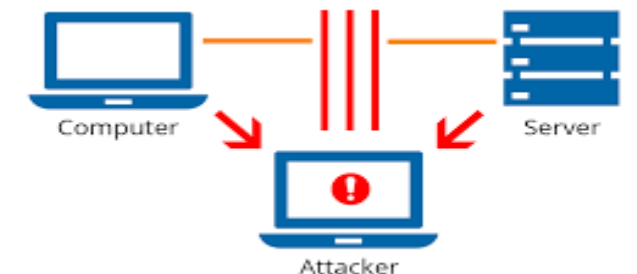


Figure 2 Microsoft Man in the middle

Kali Linux [5] is a penetration testing kit used extensively through out this project. Kali Linux is devoted to exploiting known vulnerabilities using tools such as RainbowCrack[6] and Aircrack[7] brute forcing passwords and Wi-Fi.

Prevention and Detection

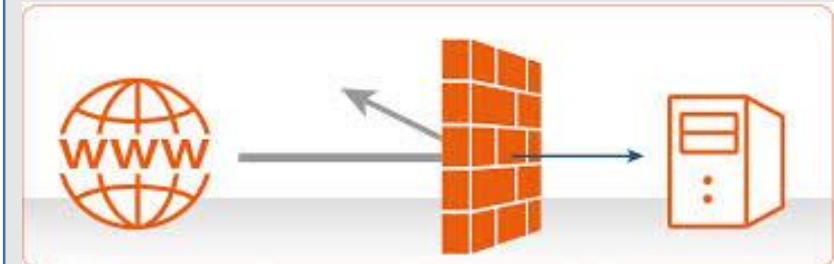


Figure.3 Ubuntu Firewall

Snort[8], an intrusion detection system and UFW[9], a firewall, will be one of a number of key security measures to protect the networks.

[1] <https://opensource.com/resources/what-open-source>

[2] <https://www.bbc.co.uk/news/uk-36239805>

[3] <https://www.gns3.com/>

[4] <http://www.vmware.com/>

[5] <https://www.kali.org/>

[6] <http://project-rainbowcrack.com/>

[7] <https://www.aircrack-ng.org/>

[8] <https://www.snort.org/>

[9] <https://help.ubuntu.com/community/UFW>