Introduction

Penetration testing is a key concept in maintaining a secure and predictable digital environment in today's massive technology ecosystem.

It is paramount that all companies test their systems, networks and devices thoroughly for vulnerabilities to avoid cyber attacks which may cause disruption to the business or even disclose personal or business-critical information.

The following walkthroughs are a compendium of penetration tests I have performed on many different machines at varying levels of personal skill as well as varying levels of technical difficulty.

Some walkthroughs may be less thorough than others as I was beginning to find my legs and learn what penetration testing methodology works best for me. (See my methodology)

I have learned a huge amount about Windows and Linux enumeration throughout this exercise and hope that reader is able to see how my knowledge in enumeration and escalation improve from host to host.

Although I was unable to gain root privilege on two of the machines (Pelagiad & Dunlain) I gave all hosts my best shot and attempted everything in my arsenal at the time of writing.

I am extremely proud of what I have achieved and am now capable of and look forward to hearing any feedback you may have.

Hayden.