OSCP-PWK – An Idiots Guide

Presented by

An Idiot

Background

- Left CIT with a BSc in Analytical Chemistry
- Worked in various labs
- Building work
- Tool hire
- Coring and chasing
- Small engine repair
- Back to CIT for the first year of the H. Dip in Cloud Computing
- Software QE at EMC

The Plan

- Pentesting With Kali linux
  - What is it?
  - What do you need for it?
  - What does it provide
  - Lab enviroment/Course material/forums
  - My experiences
  - Suggested pre-requistes (AKA What I should have known)
- Q&A
- Demo
- Q&A

What is PWK?

- Online penetration testing course
- Run by Offensive Security – the crew behind Kali Linux
- Leads to the Offensive Security Certified Professional certification
- Full details here: https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

What do you need for PWK?

- A non-free email – Work/College/Own domain
- A solid internet connection – You must pass a connection test before they will take payment
- Money – Lab access must be purchased – course material & exam fee included in first 30 day chunk
- Ability to run Kali Linux VM
- Sheer, bloody minded, stubborness

What does PWK provide?

- Access to the PWK Lab enviroment
- Tailored Kali VM
- Windows 7 Client VM with a variety of uses
- Course material via PDF and Videos
- Access to dedicated course forums
- Words to live by: **Try Harder!**

The Lab Environment

- A set of Virtual Machines configured to mimic a real life company environment
- The couse work requires you to carry out a penetration test of this environment and reporting on it.
- A report on the course activities and lab machines can be submited and will contribute to the certification exam.
- Lab is divided into multiple segments, only 1 of which is initially routable.

Course Material

- Basics of penetration testing covered via
  - A 375 page PDF
  - Video version with demonstrations
- Covers a wide range of topics:
  - Kali/Bash/Python basics
  - Tools/Information gathering
  - Buffer overflows/exploits/file transfers
  - Privilege escalation/Tunneling
  - Metasploit Framework
  - Putting it all together
  - Also contains course work which contributes to exam results

Forums

- Dedicated to the PWK course
- Allow a way of getting a nudge in the right direction or asking a few questions
- Forums are kept spolier free
- Contains errata & common issues section
- Fantastic walk through of Alpha
- It is possible to contact support staff for guidance, but their preference is that you Try Harder

My Experiences

- So far its been an overwhelming positive experience
- Very professional: All queries/problems were dealt with quickly and efficiently
- This course doesn’t really teach, it forces you to learn
- My knowledge base going in was way too low
  - Resulted in me signing up for longer lab extensions
  - Would proably have benefited from more research/learning before signing up

My Suggested Pre-requistes

(AKA What I should have known)

- Good note taking skills and software.
- Good working knowledge of
  - Basic tools: Ncat/Netcat, Wireshark, NMAP, nikto, SSH/PLINK, Msfvenom, shell spawning
  - Linux and Windows cli
  - Python/Bash/C – esp cross compiling for C
  - Metasploit Framework
  - Networking
  - Basics of Webattacks – LFI, RFI, XSS, SQL Injection
  - Basics of Webservers/services: PHP/JS/IIS/APACHE/nginx/etc
- Cheatsheets
  - Bash/NC/MSF/VI/NMAP/Spawning shells

Resources

Offensive Security PWK:

https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

Cheatsheets:

Shells: https://netsec.ws/?p=337
Linux PE:https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
Windows PE: https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
NC: https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
NMAP: https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.0.pdf
BASH: https://learncodethehardway.org/unix/bash_cheat_sheet.pdf
Reverse Shell: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Kali reference book:

http://zempirians.com/ebooks/Packt.Kali.Linux.Cookbook.Oct.2013.ISBN.1783289597.pdf