HACKING LABS – TESTY PENETRACYJNE

I. KOFIGURACJA ŚRODOWISKA DO ĆWICZEŃ Z ZAKRESU TESTÓW PENETRACYJNYCH:

1. Zainstaluj VirtualBox: https://www.virtualbox.org/wiki/Downloads
2. Pobierz **Kali Linux z Kali.org**: http://www.kali.org/downloads/
   iso32bit: http://cdimage.kali.org/kali-2.0/kali-linux-2.0-i386.iso
3. Pobierz maszynę podatną na ataki Metasploitem – **Metasploitable VMDK**:
   http://www.cs.put.poznan.pl/mmilostan/ge/laboratoria/hackinglab/metasploitable-linux-2.0.0.zip
4. Utwórz **dwie maszyny wirtualne** (Metasploitable i Kali Linux) – jedną dla Kali, drugą dla Metasploitable
5. Uruchom Kali Linux na maszynie wirtualnej jako **LiveCD** (opcjonalnie można zainstalować, ale to dość długo trwa)
6. Uruchom maszyny **Metasploitable i Kali Linux** (ta druga jako LiveCd) w VirtualBox (sieć najlepiej ustawić na HOST only, albo internal albo NAT Network).

II.ZASADNICZA CZĘŚĆ ĆWICZEŃ:

1. Zainicjalizuj instalacje **OpenVAS-a** – będzie miał do pobrania ponad 30k pluginów i może to robić w trakcie, gdy będziesz realizował pozostałe ćwiczenia. Zobacz Step 1 w instrukcji:
   http://uwnthesis.wordpress.com/2013/08/31/kali-openvas-vulnerability-scanner-how-to-use-openvas-on-kali-debian-linux/
2. Przeskanuj maszynę Metasploitable z Kali Linux przy użyciu **nmap**-a z konsoli systemowej – spróbuj użyć zaawansowanych opcji z rozpoznawaniem usług i rozpoznawniem systemu operacyjnego (zobacz: man nmap), wyniki zapisz do pliku.
3. Przeskanuj host Metasploitable przy użyciu **nikto**.
4. Uruchom metasploita:
   mfsconsole i spróbuj znaleźć exploity w bazie **MetaSploita**, których można użyć do przełamania zabezpieczeń usług zidentyfikowanych przy użyciu nmap-a i innych narzędzi (np. telnet-a, przegladarki internetowej)np.

```
#> msfconsole
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf  exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.....
```

```
msf  exploit(unreal_ircd_3281_backdoor) > exploit
```

5. Spróbuj użyć innych metod do znalezienie podatności i przejęcia maszyny metasploitable (ew. wykorzystaj podpowiedzi dostępne pod adresem podanym na końcu niniejszego pliku).
6. Spróbuj użyć OpenVAS (zainstalowanego na Kali Linux) do automatycznego przetestowania maszyny. Skorzystaj z tej instrukcji: http://uwnthesis.wordpress.com/2013/08/31/kali-openvas-vulnerability-scanner-how-to-use-openvas-on-kali-debian-linux/
7. Zobacz jakie jeszcze narzędzia są dostępne w Kali Linux.

III. NESSUS(ZADANIE DOMOWE DLA CHĘTNYCH)

1. Zainstaluj nessus-a pod Kali Linux tak jak pokazano tutaj: http://uwnthesis.wordpress.com/2013/07/31/kali-how-to-install-nessus-on-kali/
2. Spróbuj użyć Nessusa (zainstalowanego na Kali Linux) do automatycznego przetestowania maszyny.

Podpowiedzi i przykładowe rozwiazania (do części II):

https://community.rapid7.com/docs/DOC-1875