Mým úkolem bylo seznámit se s linuxem Damn Vulnerable Linux, vyzkoušet různé druhy útoků a seznámit se různými programy pro mapování prostředí, útoky a atd. K dispozici byl server s DVL, s již nahraným “děravým“ systémem. Pro rychlejší odezvu jsem si nahrál DVL na vlastní počítač. ISO obraz má něco kolem 1.5GB. A je zdarma ke stáhnutí.

Seznámení se systémem

V nabídce start je záložka Damn Vulnerable Linux, která obsahuje podnabídku

Ethical hacking
Training material
Development
Tools
Valuable websites

Ethical hacking

obsahuje mimo jiné nabídku ***Network mapping*** se spoustou programů pro mapování prostředí sítě. Asi nejznámější **nmap**, který jsem použil i já pro zjištění, které porty jsou otevřené.

Výpis programu nmap pro zjištění otevřených portů na VDL s IPv4 adresou 192.168.0.23

```
dvl3 ~ # nmap -sS -P0 -f -n -O -T 3 192.168.0.23

Starting Nmap 4.20 ( http://insecure.org ) at 2010-04-28 10:31 GMT
Interesting ports on 192.168.0.23:
Not shown: 1693 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
631/tcp  open  ipp
3306/tcp open  mysql
6000/tcp open  X11
No exact OS matches for host (If you know what OS is running on it,
```

Další program, tentokrát i s grafickým prostředím pro mapování sítě je **autoscan.** Dokáže definovat, které služby jsou aktivní, popřípadě i firewall. Nabídka Network mapping obsahuje mnoho programů a stačí si vybrat. Většina však plní stejnou funkci.

Další podnabídka je ***Penetration***. Obsahuje velice známy program **metaspoit** a to ve verzi 2 a 3. Má jak grafické prostředí, tak i webové a konzolové. Program obsahuje různé druhy útoků na známé chyby. Lze jej aktualizovat. Program je velice intuitivní stačí zjistit, třeba pomocí nmap běžící služby a již stačí vybrat exploit a nastavit cíl útoku a exploit se vykoná! Exploit je automatizovaný a pokud se se vykoná, vrátí Vám třeba konsoli s root uživatelem.

Další program, spíše database je **Milw0rm**. Jedná se o největší volnou databázi s exploitami. Mnoho programů využívá tuto databázi. Lze jej naimplementovat do matasploitu.

A poslední program **ninja**. Tento program je kombinací milw0rm a nmap. Automaticky zmapuje cíl, zjistí běžící služby a možné útoky. Z databáze vybere všechny exploity, které by mohly mít za následek průnik do počítače a použije je.

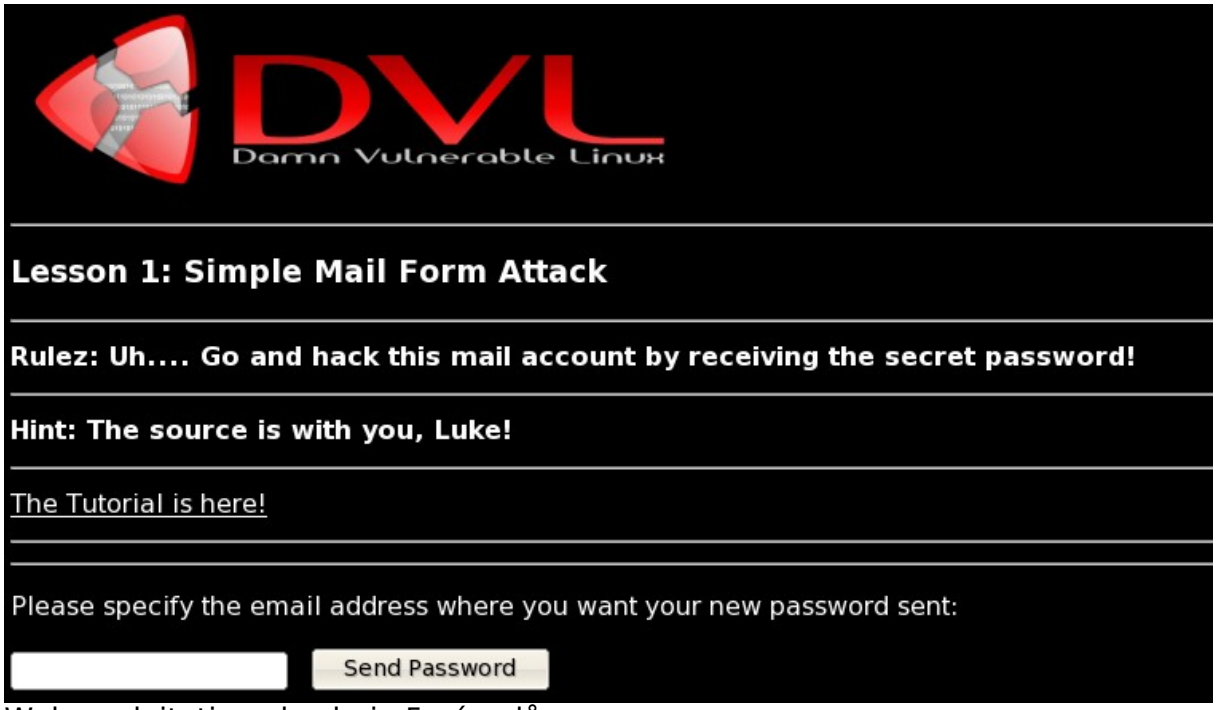
Závěr

Vyzkoušel jsem mnoho programů pro mapování prostřední a programů pro útok. Podařilo se mi hacknout WEP šifrování a pomocí matasploitu i windows XP bez firewallu a aktualizací. Nicméně VDL nikoliv.

Training material

Již z názvu je jasné, že nabídka Training material obsahuje různé materiály a návody. Asi nejzajímavější pro mne bylo podnabídka Web exploitation s názornými ukázky a návody. Jedná se o webový návod, nutností je mít zaplý mySQL a třeba appache.

Obrázek ukázky návodu pro jednoduchý útok.



Web exploitation obsahuje 5 návodů.

PORT 631 – Information

Port Number: 631

TCP / UDP: UDP

Delivery: No

Protocol / Name: ipp

Port Description: Internet Printing Protocol.