Metasploit and Armitage

Szabó Attila

Metasploit Framework

securITeam

- History (created in 2003, acquired by Rapid7 in 2009
- https://en.wikipedia.org/wiki/Metasploit_Project
- Big database of exploits and payloads
  - more than 1200 exploits
- Free, open-source
  - there are more editions: pro, expres, etc.
  - http://www.rapid7.com/products/metasploit/editions.jsp
- Console mode

Easy hacking

securITeam

- More than a database
  - infrastructure, customizable for your needs
- Manual usage
  - Scan targets and check for vulnerabilities
  - Choose exploit
  - Setup parameters and payload
  - Execute
  - Enjoy

Armitage

- Great GUI for MSF
  - front-end but also scriptable
- Integrated in Kali
- Built-in scanning
  - nmap, OS detection
  - port scan
- Automatically recommended attacks
- Post Exploitation

Starting up MSF in Kali 2.0

securITeam

- Start the Postgresql Database

  service postgresql start

- Initialize the Metasploit Framework Database

  msfdb init

- Start Armitage

  armitage

Demo

- Metasploitable 2.0
  - *http://sourceforge.net/projects/metasploitable/files/Metasploitable2*
- “Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. “

  Never expose this VM to an untrusted network (use NAT or Host-only mode)

Tutorials and links

https://www.ethicalhacker.net/features/special-events/free-armitage-and-metasploit-video-training

http://blog.cobaltstrike.com/2013/02/06/getting-started-with-armitage-and-the-metasploit-framework-2013/

https://www.offensive-security.com/metasploit-unleashed/

https://www.exploit-db.com/docs/17910.pdf