Metasploit Framework

Introduction

Agenda

- Metasploit Introduction
- Metasploit Core
  - Interface
    - MSFConsole
    - MSFCLI
    - MSFVenom
    - MSfGUI
    - MSFWeb/MSFPro
    - Armitage
    - Cobalt Strike

Agenda

- Metasploit Core
  - modules
    - exploits
    - payloads
    - auxiliary
    - encoders
    - nops
    - post
  - databases
  - meterpreter

Agenda

- MSFconsole
  - MSFConsole Basics
    - Core Commands
      - Search, Use, set/unset, show, info, route, quit/ exit
    - Database Backend Commands
    - Exploit Commands
    - Payload Commands
    - Auxiliary Commands
    - Post Commands

Agenda

- Metasploit Standard Usage
  - Information Gathering
  - Scanning
    - Network Scanning
    - Port Scanning
    - Vulnerability Scanning
  - Exploitation: Gaining Access
  - Post-Exploitation
    - Privileged Escalation

Agenda

- Metasploit Standard Usage
  - Post-Exploitation
    - Kill AV and Firewall
    - Impersonation
    - Keylogging and Sniffer Extensions
    - Backdoors
    - Port Forwarding
    - Network Pivoting

Agenda

- Metasploit Advanced Usage
  - Client Side Attacks
    - Binary Payloads
    - Client Side Exploits
  - Meterpreter Scripting
  - Mimikatz
  - Create Metasploit Module

Introduction

METASPLOIT FRAMEWORK

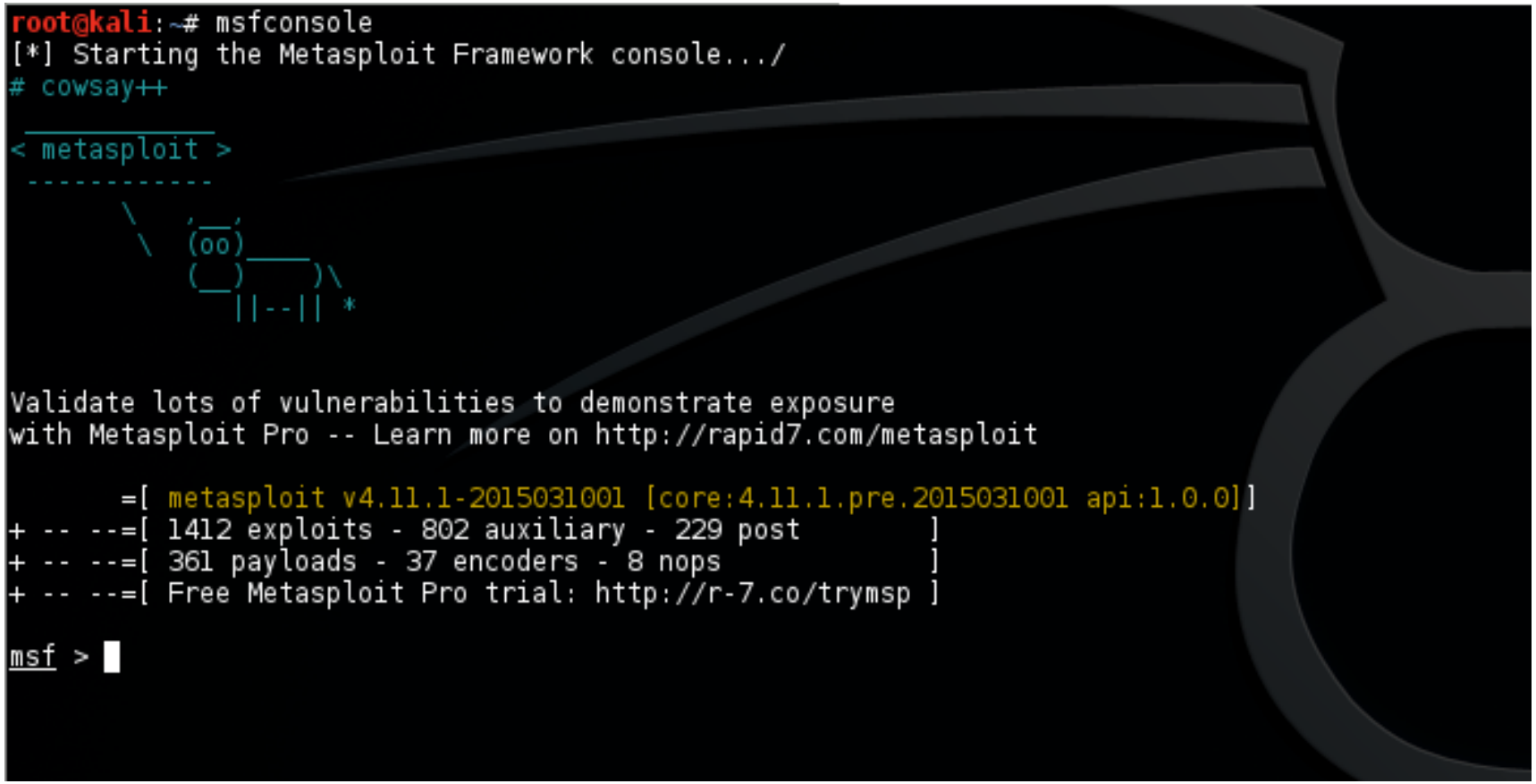
Metasploit Framework

- Created by HD Moore in 2003
- Written in Perl and only with 11 exploits
- Rewritten in Ruby, Msf 3.0, 2007
- 2009, Acquired by Rapid7 but still free and open source

Metasploit Framework

- Lebih dari hanya sekumpulan exploit atau payload.
- Selalu di update dan di maintain
- Sangat mendukung kustomisasi, penulisan ulang
- Sangat mendukung kegiatan pentest, riset terkait exploitasi
- …

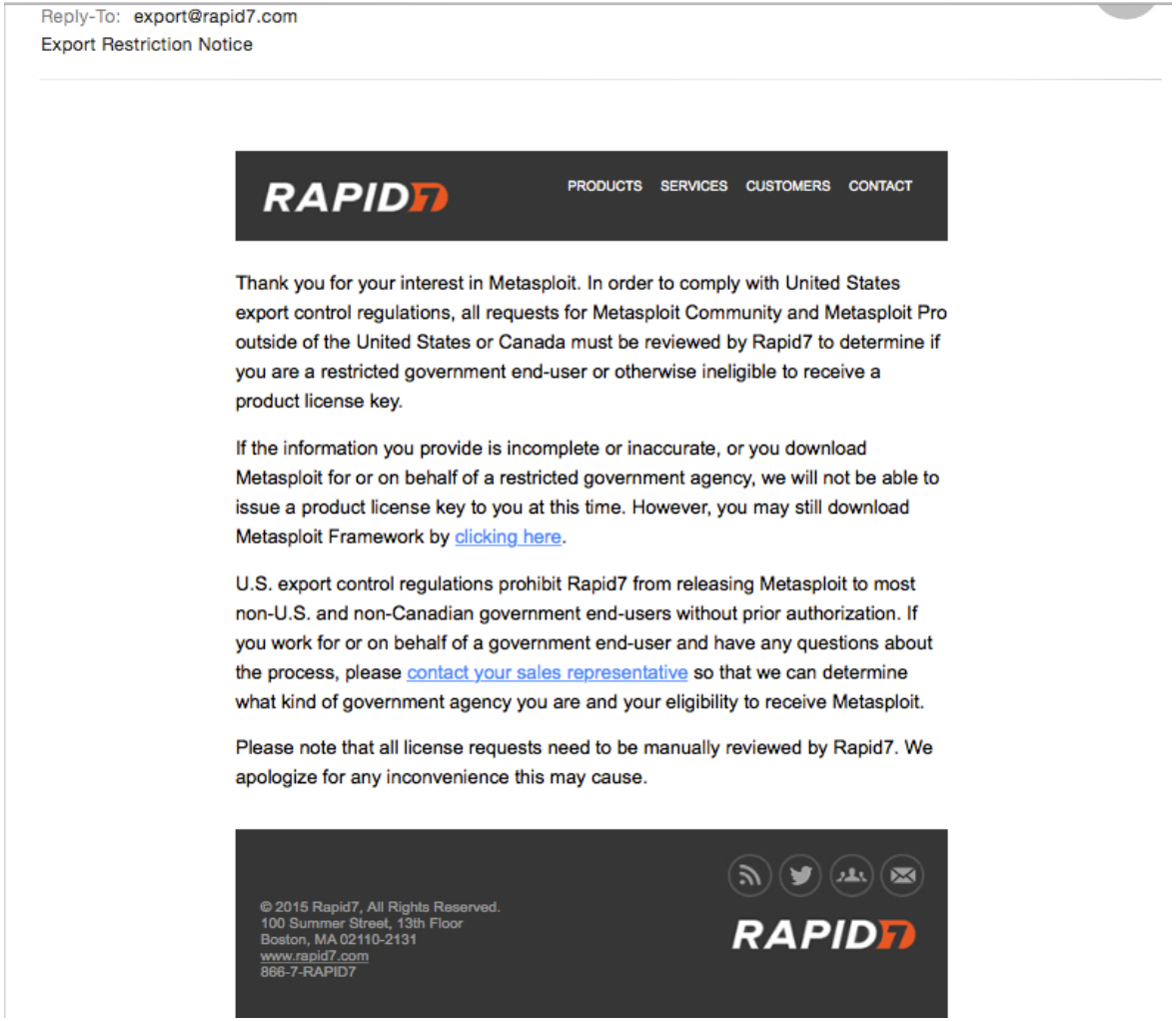
Metasploit Framework



Metasploit Framework

- download: http://www.metasploit.com/
- community: https://community.rapid7.com/community/metasploit

Metasploit Framework



Reply-To: export@rapid7.com
Export Restriction Notice

RAPID7 PRODUCTS SERVICES CUSTOMERS CONTACT

Thank you for your interest in Metasploit. In order to comply with United States export control regulations, all requests for Metasploit Community and Metasploit Pro outside of the United States or Canada must be reviewed by Rapid7 to determine if you are a restricted government end-user or otherwise ineligible to receive a product license key.

If the information you provide is incomplete or inaccurate, or you download Metasploit for or on behalf of a restricted government agency, we will not be able to issue a product license key to you at this time. However, you may still download Metasploit Framework by clicking here.

U.S. export control regulations prohibit Rapid7 from releasing Metasploit to most non-U.S. and non-Canadian government end-users without prior authorization. If you work for or on behalf of a government end-user and have any questions about the process, please contact your sales representative so that we can determine what kind of government agency you are and your eligibility to receive Metasploit.

Please note that all license requests need to be manually reviewed by Rapid7. We apologize for any inconvenience this may cause.

100 Summer Street, 13th Floor
Boston, MA 02110-2131
www.rapid7.com
866-7-RAPID7

RAPID7

References

- Metasploit: The Penetration Testing Guide - David kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
- Mastering Metasploit - Nispun Jarwal
- Metasploit Unleashed - Offensive Security - http://www.offensive-security.com/metasploit-unleashed
- Securitytube Metasploit Framework - http://www.securitytube.net
- Post Exploitation Using Meterpreter - Shubham Mittal - https://www.exploit-db.com/docs/18229.pdf

Questions?

Metasploit Framework

Introduction