Metasploit

Jay Turla (@shipcod3)

#! whoami

- Application Security Engineer at Bugcrowd Inc.
- One of the goons of ROOTCON – the premiere hacking conference in the Philippines
- Former Senior Security Consultant at Hewlett-Packard Enterprise (Fortify on Demand)
- Acknowledged and rewarded by Facebook, Adobe, Yahoo, Microsoft, Mozilla, etc. for his responsible disclosures
- Contributed auxiliary and exploit modules to the Metasploit Framework: Host Header Injection Detection, BisonWare BisonFTP Server Buffer Overflow, Zemra Botnet CnC Web Panel Remote Code Execution, Simple Backdoor Shell Remote Code Execution, w3tw0rk / Pitbul IRC Bot Remote Code Execution, etc.

bugcrowd

Disclaimer

- Some humor images / memes may have explicit language in them

Topic Outline

- Introduction to Metasploit Framework
- Metasploit Interfaces
- Replication Steps / Prerequisites
- Metasploit Basics (msfconsole only - no other interfaces)
- Demo (but if we have time we go for Armitage)
- References

Metasploit Framework

- One of the most popular open source penetration testing tools / frameworks the world has ever known
- Metasploit / MSF was created by H. D. Moore in 2003 as a portable network tool using Perl.
- By 2007, the MSF had been completely rewritten in Ruby.
- The project was acquired by Rapid 7 in 2009
- Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary editions called Metasploit Express and Metasploit Pro.

Metasploit Interfaces

- **Metasploit Framework Edition** - the command-line interface and also a free version (msfconsole)
- **Metasploit Community Edition**- a free, web-based user interface for Metasploit
- **Metasploit Express**- open-core commercial edition for security teams who need to verify vulnerabilities
- **Metasploit Pro** - open-core commercial Metasploit edition for penetration testers
- **Armitage** - free graphical cyber attack management tool for the msg (not maintained by Rapid 7)
- **Cobalt Strike** - collection of threat emulation tools provided by Strategic Cyber LLC to work with the msf. Includes all features of Armitage and adds post-exploitation tools, in addition to report generation features.

bonus points lol

bugcrowd

why we need msfconsole for this one?

bugcrowd

Prerequisites

- Kali Linux / any other pen testing distro that has msf
- Windows XP Service Pack 3
- Metasploitable 2
- Virtual Machine (yeah interface with them)
- Understand Linux
- Stop being a script kiddie - seriously
- Use google if you need any help or ask some of your friends

seriously no!

bugcrowd

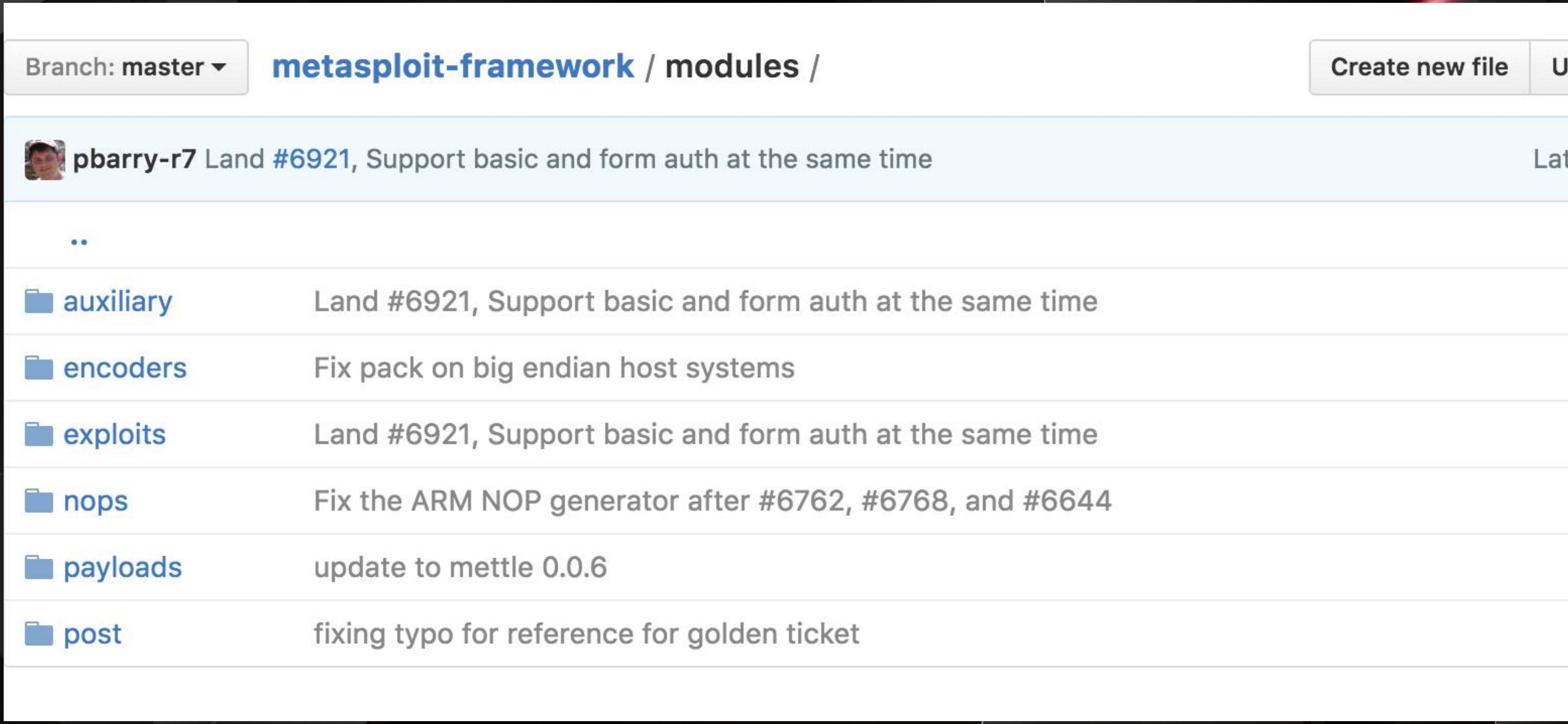
Don’t rely on Hail Mary Attacks

bugcrowd

Starting it all up

- *msfupdate*
- *service postgresql start*
- *msfdb init*
- *msfrpcd -P msf*
- *msfconsole*
- *help*

The Modules - let’s define them



metasploit-framework / modules /

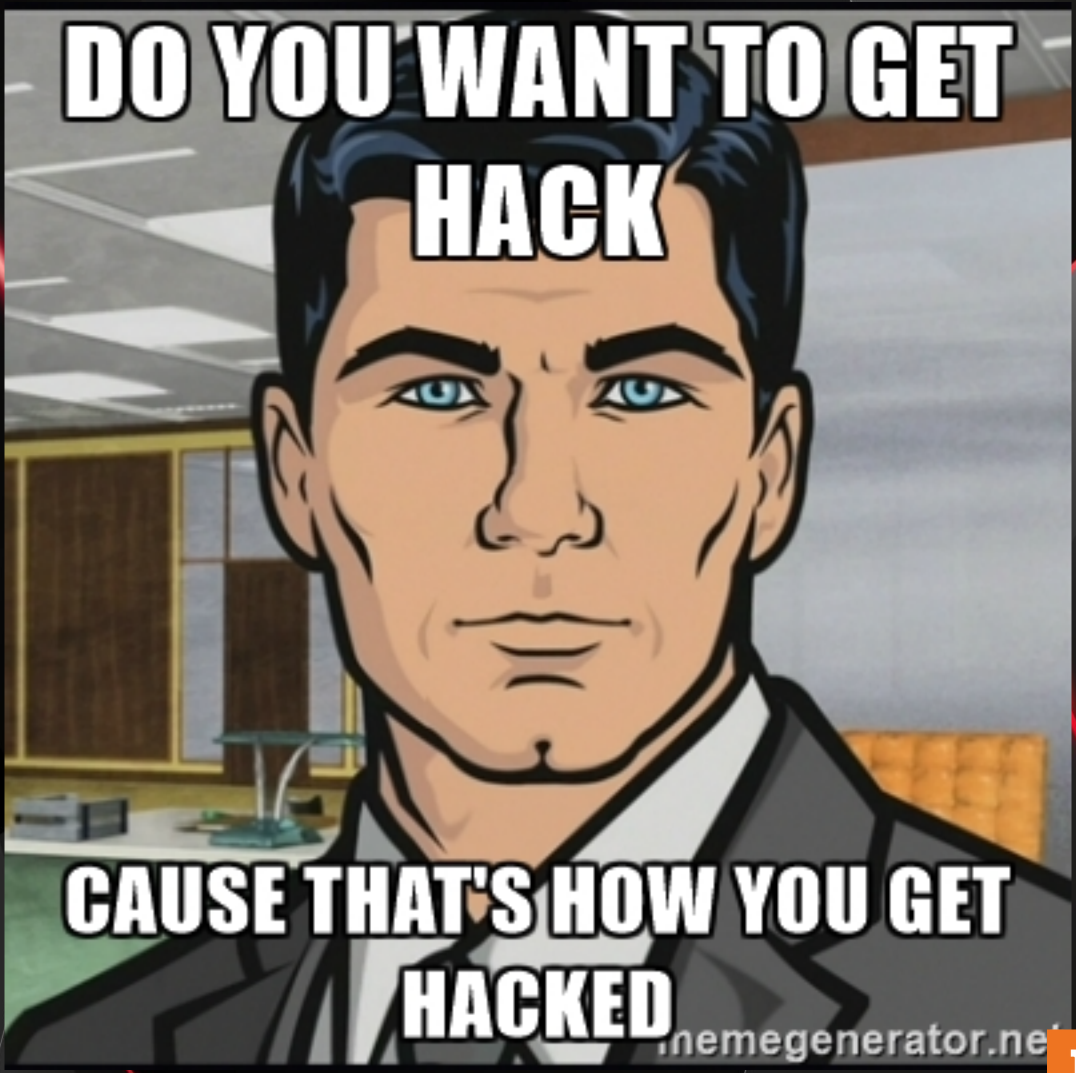
pbarry-r7 Land #6921, Support basic and form auth at the same time

..

auxiliary	Land #6921, Support basic and form auth at the same time
encoders	Fix pack on big endian host systems
exploits	Land #6921, Support basic and form auth at the same time
nops	Fix the ARM NOP generator after #6762, #6768, and #6644
payloads	update to mettle 0.0.6
post	fixing typo for reference for golden ticket

bugcrowd

Demo



bugcrowd

References

- http://docs.kali.org/general-use/starting-metasploit-framework-in-kali (Kali Documentation)
- https://en.wikipedia.org/wiki/Metasploit_Project (History)
- https://github.com/rapid7/metasploit-framework/ (Official Repo)
- https://www.offensive-security.com/metasploit-unleashed/ (kinda old actually so use at your own risk)
- Brain – stock knowledge