

Cheddar Horsemen - Capture the Flag Training  
2nd September, 2011  
Level 1, 126 Margaret St., Brisbane

# Introduction to Metasploit

Nishchal Kush  
Information Security Institute, Queensland University of Technology  
[n.kush@qut.edu.au](mailto:n.kush@qut.edu.au)



a university for the **real** world<sup>®</sup>

CRICOS No. 00213J

# Disclaimer



- Am not l337
- Not authorised
- Do not try this at home

Image: <http://andrewpavelski.com/2011/08/19/the-three-shades-of-seo-white-hat-grey-hat-black-hat/>



a university for the **real** world<sup>®</sup>

2

Introduction to Metasploit

CRICOS No. 00213J

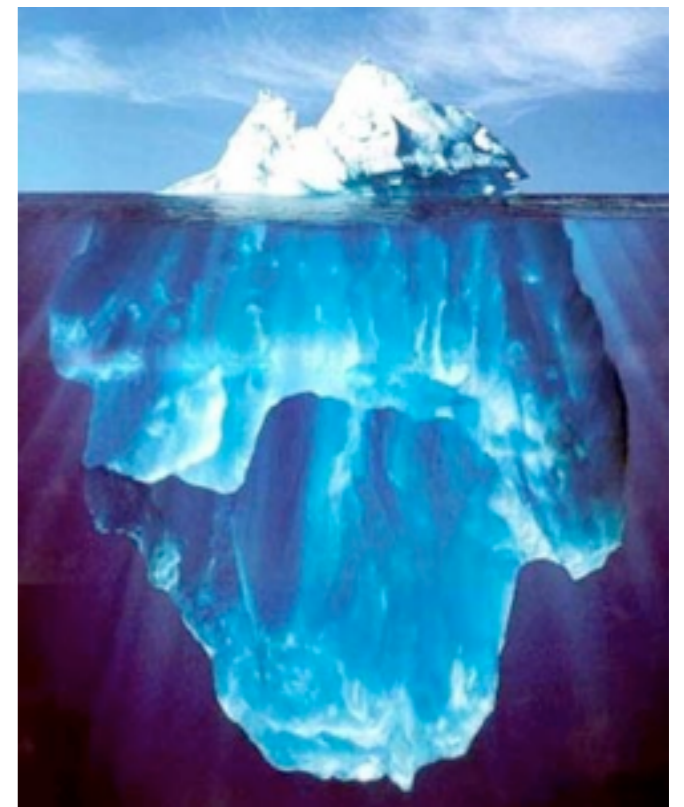
Friday, 2 September 2011

- Am not a hacker.
- Am not a metasploit expert.
- Am not recommending people test metasploit in the wild.
- Do not test on a network/system that you do not own.

2

# Outline

- Introduction to Metasploit
- Set-up
- Demonstration



[http://www.dadalos.org/frieden\\_int/grundkurs\\_4/eisberg.htm](http://www.dadalos.org/frieden_int/grundkurs_4/eisberg.htm)

# Introduction to Metasploit

- H D Moore
- Rapid7
- Penetration testing tool
- De-facto standard

- Developed by H D Moore, mostly Ruby code,
- De-facto standard because its platform independent, good collection of exploits
- Community version, professional version has more automation built in

# Metasploit

- Modules
  - exploits and payloads
- Allows automation
  - autopwn w/ Nessus
- Metasploit Training
  - <http://www.offensive-security.com/>

- Exploit mostly for windows, get more exploit code and automation in paid versions
- Modules effectiveness is ranked in metasploit console
- Autopwn can be difficult to configure.
- Metasploit Unleashed gives an excellent tutorial, also check you tube

# Installation

- <https://community.rapid7.com/community/metasploit>
- <http://nkush.blogspot.com/2011/09/installing-metasploit-400-on-apple-mac.html>



Image: <http://harmonytimberfloors.com/installation.php>

- can be simple to install
- more involved steps for additional functionality

# msfconsole (show msfconsole\*)

- back
- check (not widely used)
- search
- use
- show options
- run/exploit



Image: <http://www.gerardribas.com/console/>



attacker

# Set-up

Mac OS X 10.6.8  
metasploit 4.0.0  
VirtualBox 4.0.12  
192.168.56.1



attacker

Mac OS X 10.6.8  
metasploit 4.0.0  
VirtualBox 4.0.12  
192.168.56.1

# Set-up

(show virtualbox\*)

Ubuntu 8.04 Server  
(metasploitable  
VMware image)  
192.168.56.???

host-only

target



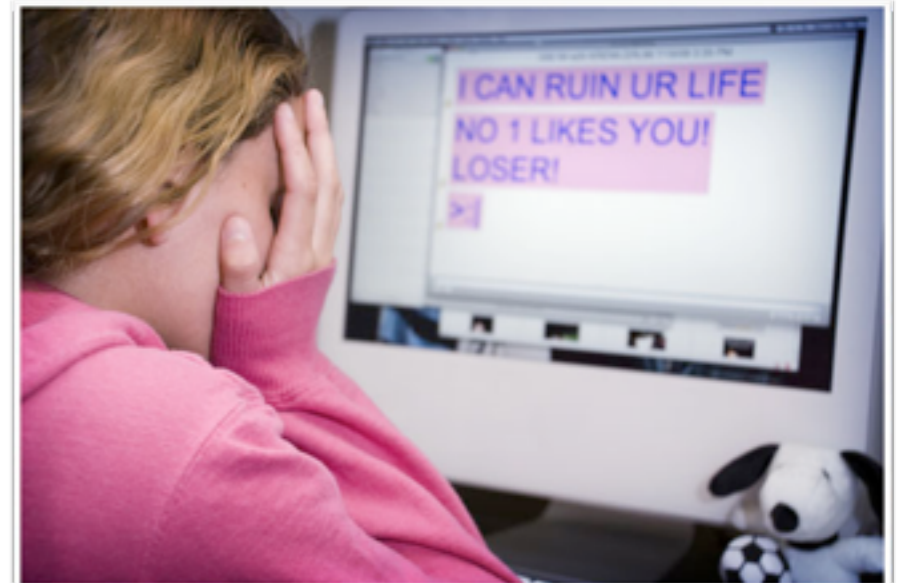
attacker

Mac OS X 10.6.8  
 metasploit 4.0.0  
 VirtualBox 4.0.12  
 192.168.56.1

# Set-up

Own

Ubuntu 8.04 Server  
 (metasploitable  
 VMware image)  
 192.168.56.???



target

Image: <http://mfjtribune.com/2011/06/04/cyber-attacks-on-us/>  
<http://internetsafetynb.wikispaces.com/>

# Requirements

- nmap
- msfconsole
- wordlist



# Service Discovery

- hping
- nessus
- metasploit!
- nmap

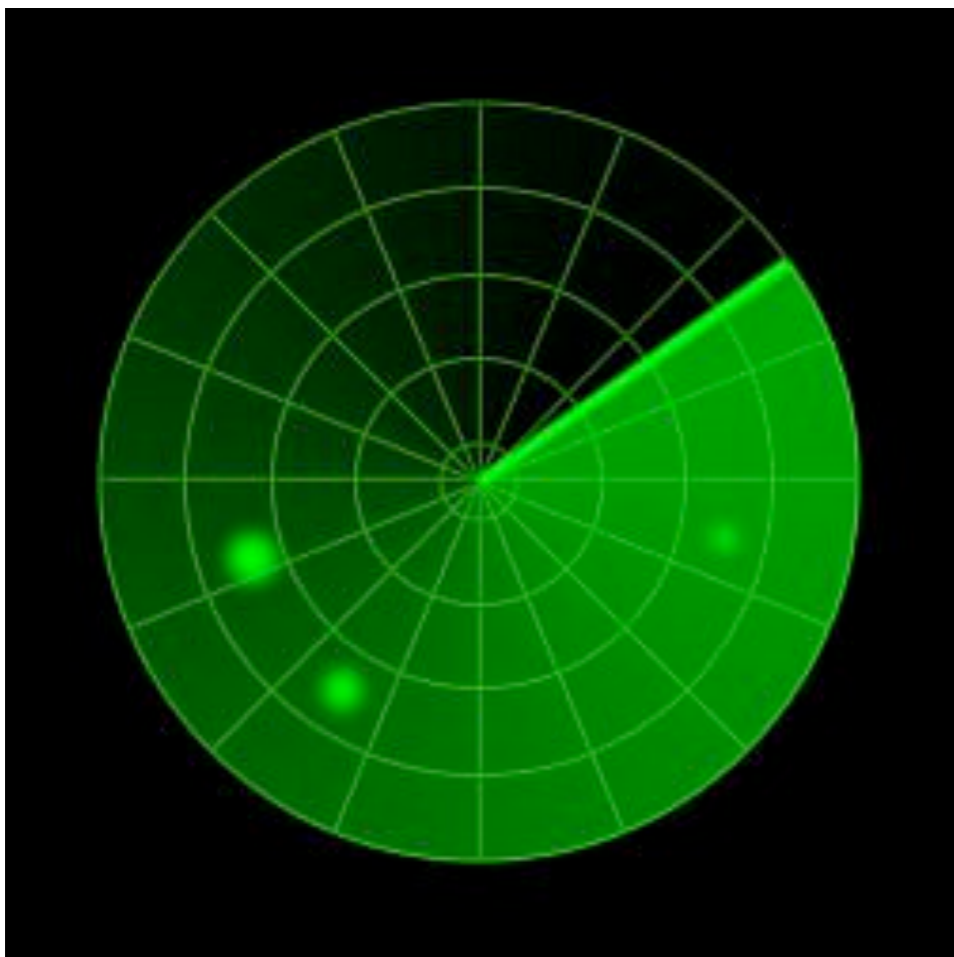


Image: <http://www.integration1.com.au/NetSecScanInfo.htm>

- hping can be troublesome
- metasploit has port scanner in it but may be show
- nmap is most comprehensive for me



# Reconnaissance

- `nmap -v -n 192.168.56.0/24`
- `nmap -v -n -sV 192.168.56.???`
- (show nmap use\*)

Image: <http://www.militarypictures.info/patches/recon.jpg.html>

- verbose, do not resolve DNS, network
- verbose, do not resolve names, service versions, host

# Exploit

- exploit [+]
- payload [\*]
- pwn [-]
- (show main demo\*)



Image: <http://forum.gnacktrack.co.uk/What-is-exploit-and-how-to-use-it-td2707057.html>

# Covering your tracks

- Clean up log files
- Meterpreter migration

# Thank you

[n.kush@qut.edu.au](mailto:n.kush@qut.edu.au)

