Inside Out Hacking – Bypassing Firewalls

St. Louis Security Group

2006-Aug-30

Christopher Byrd, CISSP
Senior Security Engineer
SAVVIS Communications

Quick Introduction

- About Me
  - Christopher Byrd, CISSP
    - Senior Security Engineer
    - chris@byrd.net
    - www.riosec.com
- About Metasploit
  - Primary developers H D Moore (hdm) and Matt Miller (skape)
  - www.metasploit.com
  - metasploit.blogspot.com

What is Metasploit (review)

- “The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code.”
- Original version written in Perl
- Modular, scriptable framework

Metasploit 3

- Written in Ruby
  - Supports Linux, BSD, MacOSX, Windows (with cygwin)
- Modular, scriptable framework
- Mixins for common protocols
  - Using mixins, exploits can be written in as few as 3 lines of code!
- Auxiliary modules

Metasploit Uses

- Metasploit is for
  - Research of exploitation techniques
  - Understanding attacker’s methods
  - IDS/IPS testing
  - Limited pentesting
  - Demos and presentations
- Metasploit isn't for
  - Script kiddies
    - Limited and “stale” exploits

Interfaces

- msfconsole
  - Interactive console interface
- msfcli
  - Command line exploitation
- msfpayload
  - Create encoded (executable) payloads
- msfweb (being reworked)
  - Because everything has to have a web interface
- msfwx GUI (in development)
  - Point, Click, 0wn
- msfapi (in development)
  - Modularized development platform

Exploits

- 148 exploits in 2.6
- 84 rewritten exploits for 3.0
- hpux / irix / linux / macosx / solaris / windows / etc…
- Application specific exploits
  - Browsers, backup, ftp, etc…
- Exploits are passive (client bugs) or active (service exploitation)
- Mostly remote exploits, no local privilege escalation (yet)
- Organized as platform/application/exploit
  - windows/browser/ms06_001_wmf_setabortproc
  - osx/samba/trans2open

Payloads

- Communication types
  - Reverse
  - Forward
  - Findtag
  - HTTP (PassiveX)
- Payload types
  - Upexec
  - Shell
  - Adduser
  - Meterpreter
- Platform/Payload/Communication
  - windows/meterpreter/reverse_http
  - linux/x86/shell/find_tag

IDS Evasion

- Encoders
  - change payload, sometimes exploit signature
- Multiple NOP (No Operation) generators
- ips_filter plugin

What's New this month

- New Website
- Metasploit 3.0 beta 2
  - New auxiliary modules
    - Sweep_udp
    - Smb_version
    - Ms06_035_mailslot
  - New exploits
    - Includes Netapi_ms06_040 (< 1 mo old)
  - Generic payloads
- Subversion access!
  - svn co http://metasploit.com/svn/framework3/trunk

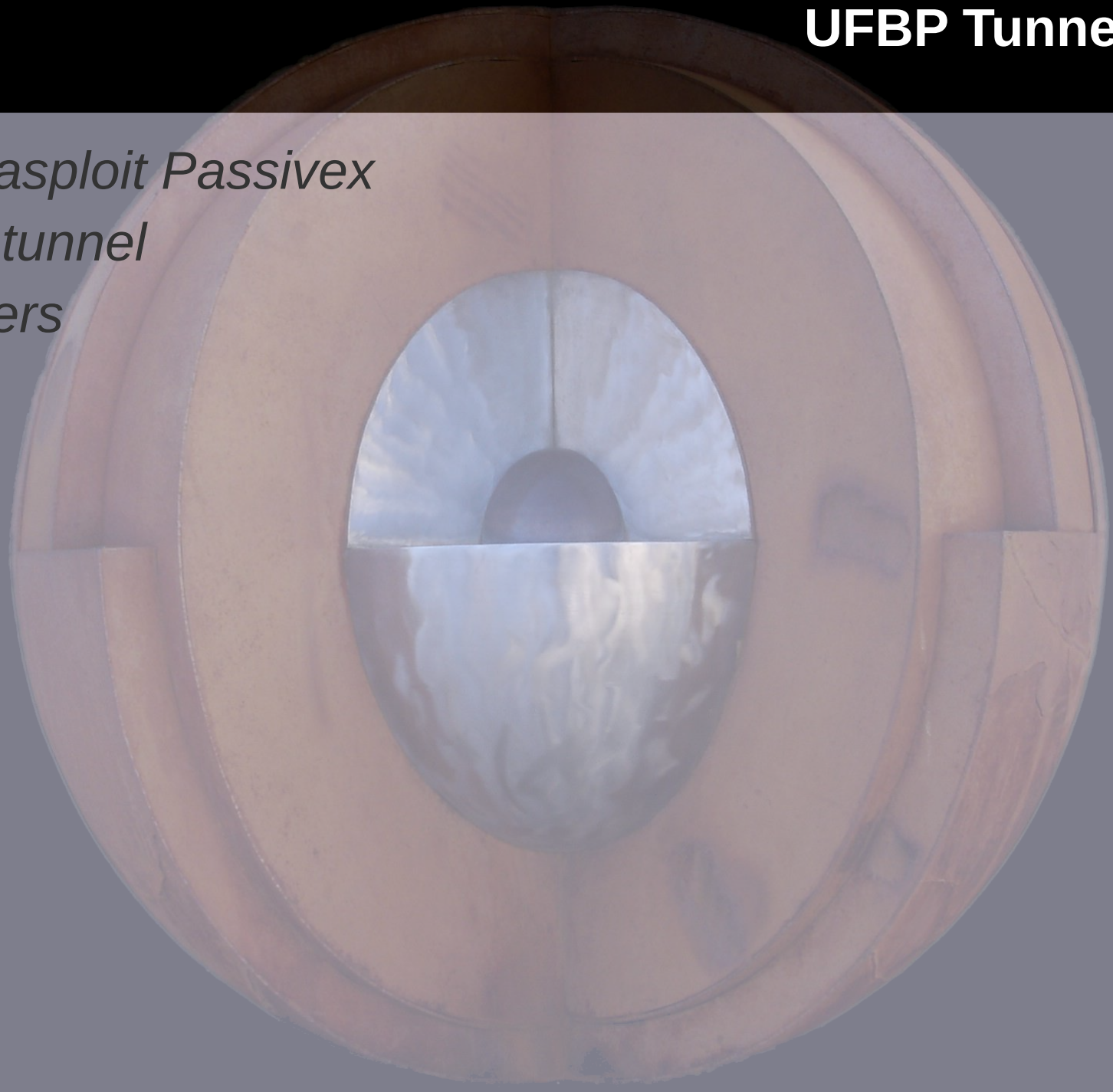
Firewalls != secure

- *Most common question I'm asked:*
  - *I have a firewall, will that protect me?*
- *Firewalls stop most "shotgun" and scanning attacks, but:*
  - *L7 attacks*
  - *Signature evasion*
  - *Client side attacks*
    - *Often used to create botnets*
  - *Human side attacks (L8)*
    - Phishing
    - Social Engineering
- Internet worms are getting rare

UFBP

- *Universal Firewall Bypass Protocol*
  - *Also known as HTTP*
- *Most companies open up outbound HTTP for web browsing*
- *Many programs (including commercial products) are using HTTP to tunnel communications*
  - *Instant Messaging*
  - *SOAP/XML*
  - *Remote desktop (GoToMyPC)*
- *These companies are using HTTP because it is almost universally allowed*
- *Inbound HTTP has to be allowed to company web servers*

UFBP Tunneling



- *Metasploit Passivex*
- *Httptunnel*
- *Others*

UFBPS Tunneling

- *Outbound HTTPS (tcp/443) allowed out for accessing secure sites*
  - *Banking*
  - *Shopping*
- *HTTPS also used to avoid restrictions*
  - *Google (cache, mail, talk)*
  - *Anonymizer services*
- *SSL encryption bypasses IDS detection*

Other related protocols

- *DNS*
  - *Nstx (ip-over-dns)*
  - *OzymanDNS*
- *ICMP (ping)*
  - *Ptunnel*
  - *itun*

Attack pivoting

- *Exploit an internal host via client side exploit*
- *Gather information on internal network*
  - *IP addresses, routes, system information, shares, etc.*
- *Route through internal client to attack other hosts*

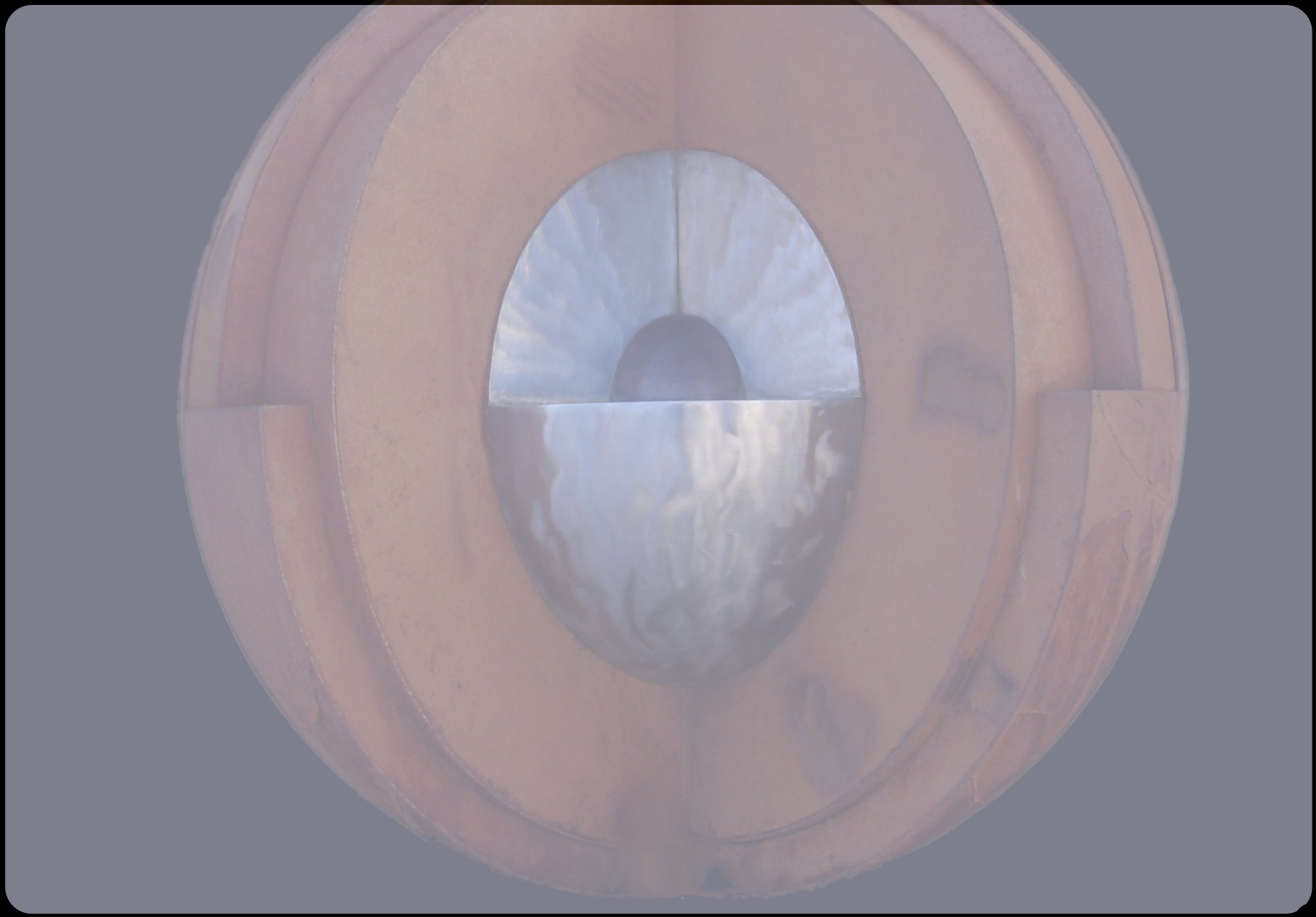
Other problems with firewalls

- If it doesn't go through the firewall, the firewall can't do anything
  - Wireless
  - VPN connected systems
- The allow any outbound rule
  - -- enough said

Anatomy of an Attack

- Victim clicks URL from email or web
  - Infected sites serves up URL in IFRAME
- Victim makes HTTP request to msf web server
- Msf web server returns wmf or other client side exploit
- PassiveX modifies registry entries on Windows to permit loading untrusted ActiveX controls
- PassiveX loads second stage ActiveX control from msf web server
- PassiveX loads payload dll (Meterpreter, VNC, etc) from attacker (tunneled over HTTP)

Demos



Blue sky: What is the solution?

- *Put the PC in a safe, disconnected from power*
- *Marcus Ranum's "Ultimately Secure Deep packet inspection and application security system"*
  - *Wirecutters*
- *Allow only limited protocols to trusted (whitelisted) connections*
- *Don't tunnel stuff over HTTP*
- *IETF ratifies secure protocols*

Real world: what helps

- *Layer 7 firewalls check for protocol conformance*
  - *Just because it goes over port 80 doesn't mean its HTTP*
- *Signatures can catch unsophisticated payloads*
  - *Host based signatures are better, as network permutations are removed*
- *Statistical analysis of traffic*
  - *Ranum's second law of Log Analysis:*
    - *The number of times an uninteresting thing happens is an interesting thing*

Quotes (because we're geeks)

- "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards." -- Gene Spafford
- "Most organizations have already given up control over outgoing traffic. What they don't realize is that, by extension, they have also given up control over incoming traffic." - Marcus Ranum
- "When you know that you're capable of dealing with whatever comes, you have the only security the world has to offer." -- Harry Browne