Zen and the Art Of An Internal Penetration Testing Program Part II

Paul Asadoorian
paul@pauldotcom.com
http://pauldotcom.com

v1.0
April-09
In Part I...

- Why we should perform internal penetration testing
- How to structure our internal program
- Quickly discover targets on the network
- Jump from discovery to exploitation
- Integrate Nmap results into Metasploit, Nessus, and Core IMPACT
- Detect rogue access points and changes in the network
- Use Nmap NSE to find vulnerabilities
Part II - Agenda

- Why should we exploit stuff?
  - What does breaking into a system prove?
- Why should we go deeper?
- What should the report look like?
Part II - Agenda (2)

Part I
- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities

Part II
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- Phase VI - Reporting
Why should we exploit vulnerabilities internally?

- Reduce false positives
- Test the internal response procedures
- Improve the integrity of the report
  - “My system isn’t vulnerable”
- “I have Host-IPS/Anti-Virus, you can’t hack me”
- “Users would never click a link…”
- “We have an IDS, we’re safe”
Why should we go deeper?

• Never know what you may find:
  – Sensitive information on a user’s desktop? GASP! That’s against the corporate policy!
  – What would happen if server1 gets hacked?

• Helps you complete the picture to determine how much effort and resources goes into defense
What should the report look like?
What should the report look like?

- After all your hard work, effort, hacking, cracking...
  - Heck, you could even write a few exploits along the way
- All someone is going to see is a report
  - I call it “Word Programming” to make myself feel better
- **Bottom line:** actions will be taken solely based on your report, so make it count
Phases

• Phase I - Target identification
• Phase II – Detect OS & Services
• Phase III – Identify Vulnerabilities
• **Phase IV – Exploitation**
• Phase V – Post-Exploitation
• Phase VI - Reporting
Exploitation

• Remote exploits
• Default username/password
  – Password brute force
• Client-side exploits
  – Yes you should run these internally
• If all else fails, MiTM
  – WPAD
  – Karmetasploit
Remote Exploits – From 1995 to today in 3 slides

• Remote exploits are a fun and easy way to pwn your way through the internal network

• People have learned to patch them and this takes much of the focus when people talk about “security”
  – Fortunately for us there are tons of other ways to be successful
Remote Exploits – All you need is one

- Typically there is at least one system that is vulnerable to a remote exploit on every network
  - Usually left behind by a vendor
  - Running software someone forgot about
  - Is a “lab” system
  - Fell out of patch cycle for a myriad of reasons
You need to Pwn and pillage

- Collect all the local hashes
- Use “incognito” to escalate privileges
- Review all local files and file shares
- All your activity should support gain information to pwn more systems and access more information quickly
- System hashes have proven most useful..
Pass Me The Hash Man

- Metasploit and Core IMPACT can both use the pass-the-hash technique
- Typically system builds will share a local Administrator account
  - Nothing drives this point home like pwning an entire subnet of desktops
- Deploy agents
  - Lots of agents
Default Username/Password

• DRAC = Dell Remote Access Controller
  – AKA DRAC-In-A-Box
• Web GUI attached to embedded system inside server
• Controls power, console access, alerts on failure (SNMP)
• Even creepier than that picture...
Console = Root

You have new mail in /var/spool/mail/root

[root@localhost network-scripts]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=root:system_u:unconfined_t:SystemLow-SystemHigh
[root@localhost network-scripts]# _
That’s Great – Now What?

- During internal penetration testing you can often gain shell on many hosts
- You need to collect information fast to analyze risk and move on
- The Core IMPACT agent is a great way to do this
Core IMPACT Agent – Not just for exploits

- Using Core IMPACT you can deploy an agent with:
  - TELNET (sudo support)
  - SSH (Password/Key)
  - Netcat ("unix|win-portshell")
  - SMB (Including Pass-The-Hash)

Information on using Pass-The-Hash technique
Metasploit – Meterpreter + Multi-Handler

• You can replicate this functionality with Metasploit
• Script the login (using language of choice, expect even?)
• Using multi-handler to wait for connections

```shell
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```
Finding Shares – Sharing is fun on the network!

• 
  ```
  # ./nessuscmd -U -p139,445 -V -i
  10396 192.168.1.0/24
  ```
• The above command will run Nessus and find all open SMB shares
• Works for Samba or Windows
• Read access leads to potential sensitive documents
  – Especially with multi-function devices, documents being scanned/faxed/copied get stored
+ Results found on 192.168.10.230:
- Port netbios-ssn (139/tcp) is open
- Port microsoft-ds (445/tcp) is open

[!] Plugin ID 10396

Synopsis:

It is possible to access a network share.

Plugin output:

The following shares can be accessed as nessus6804946061421403042121321 621:

- backup - (readable,writable)
  + Content of this share:
    ..
    CreditApplication_Fax.pdf
    Payroll_2009.xls
    Invoice10001.doc
Phases

• Phase I - Target identification
• Phase II – Detect OS & Services
• Phase III – Identify Vulnerabilities
• Phase IV – Exploitation
• Phase V – Post-Exploitation
• Phase VI - Reporting
Post-Exploitation

- Finding the sensitive information
- Collecting host information
  - Network/system
  - Password hashes
- Capturing data
  - Screen
  - Video
  - Audio
  - Keystrokes
  - Memory contents
Finding Sensitive Information

• Things to look for:
  – Files labeled “Backup” or archived files
  – SSH keys
  – Office documents containing passwords
  – Text dumps of the database
  – Files on the user’s desktop, especially text files labeled “passwords.txt”
  – Web browser history, finds more targets
  – RDP (Terminal Services) client history

Check out Mike Poor’s presentation on this topic here:
Collecting Information From The Operating System

- Winenum is a meterpreter script to automate this
- Windows:
  - Wmic
  - Netstat/route
  - “net” command
  - Registry
- Linux
  - Netstat, route
  - /etc/hosts

```ruby
# Commands that will be ran on the Target commands = [
  'cmd.exe /c set',
  'arp -a',
  'ipconfig /all',
  'ipconfig /displaydns',
  'route print',
  'net view',
  'netstat -nao',
  'netstat -vb',
  'netstat -ns',
  'net accounts',
  'net accounts /domain',
  'net session',
  'net share',
  'net group',
  'net user',
  'net localgroup',
  'net localgroup administrators',
  'net group administrators',
  'net view /domain',
  'netsh firewall show config',
  'tasklist /svc',
  'tasklist /m'
]```
Winenum – Sample Output

Date: 2009-02-23 12:19:37
Running as: CORE-IMP\john
Host: CORE-IMP
OS: Windows XP (Build 2600, Service Pack 3).

*******************************************************************************
  Output of cmd.exe /c set
*******************************************************************************
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\john\Application Data
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=CORE-IMP
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=C:\Documents and Settings\john
J2D_D3D=false
LOGONSERVER=\CORE-IMP
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATH Ext=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 6, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=1706
ProgramFiles=C:\Program Files
PROMPT=$P$G
Darkoperator Meterpreter Scripts

• They can all be found at:

• Three you want to use on every test:
  – Keylogger:
    • http://www.darkoperator.com/meterpreter/keylogrecorder.rb
  – Memory Dump:
    • http://www.darkoperator.com/meterpreter/memdump.rb
  – Sound recorder:
    • http://www.darkoperator.com/meterpreter/soundrecorder.zip
Useful Information Gathered From Meterpreter Scripts

- **Keylogger**
  - Passwords (Even to *other* systems)
  - General information (Email, chat)

- **Memory**
  - Encryption keys
  - Other encrypted data

- **Sound recorder**
  - Reconnaissance tool, example 900Mhz cordless phone sniffing
Screen Capture

- Oh how we love pretty pictures
- Core IMPACT – Built-in Module
- Metasploit – Meterpreter script
- They work great to drive a point home in the report
- You can learn A LOT about the host you compromised...
Or sometimes not so much...
Smile, You’re On Pen Test Camera!
Ethackal – Video Capture

- Useful to see if the user is actively using the computer, or stealthily capture what they are up to
- Uses Meterpreter to upload a small 3rd party program to capture movie
- Takes movies in short bursts, configurable time lengths
- Download here:
Capturing Is Stealthy, but..

- Sometimes you just need to interact with the host
- Reason: Demonstrate Risk
- Caution!
  - User’s may notice when you start moving their mouse
  - Remove when done
- Two primary ways:
  - VNC (Good OS Support)
  - RDP (Built-in to most versions of Windows)
  - Example...
<table>
<thead>
<tr>
<th>Title</th>
<th>Artist</th>
<th>Time</th>
<th>Year</th>
<th>Catg</th>
<th>Swprs</th>
<th>Prmos</th>
<th>BEDS</th>
<th>SFK</th>
<th>PSA's</th>
<th>MusTitle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Just What I Needed</td>
<td>The Cars</td>
<td>00:03:39</td>
<td>105</td>
<td>0540</td>
<td>12:28:12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mississippi Queen</td>
<td>Mountain</td>
<td>00:02:27</td>
<td>105</td>
<td>0526</td>
<td>12:32:46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brace Your Self</td>
<td></td>
<td>00:00:11</td>
<td>SWE</td>
<td>0000</td>
<td>12:35:15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>They Might Be Giants</td>
<td>They Might Be Giant</td>
<td>00:02:26</td>
<td>107</td>
<td>0779</td>
<td>12:35:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stupid Girl</td>
<td>Garbage</td>
<td>00:04:22</td>
<td>107</td>
<td>02020</td>
<td>12:37:56</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I Alone</td>
<td>Live</td>
<td>00:03:55</td>
<td>107</td>
<td>0104</td>
<td>12:42:13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Zen and the Art of an Internal Pen Testing Program – Part II**

- A box full of sharp ob Used
  - (107)0151  2:54 2004
- A Change of Scene
  - Citizens Here and Abr:
  - (110)0518  4:03 2004
- A Cold Day in Hell
  - Time Machine
  - (101)0155  2:57
- A Day in the Life
  - Beatles
  - (105)0403  4:37 2004
- A Favor House
  - Atlantic
  - Cohed and Cambria
  - (110)0394  3:44 2004
- A Harpoon
  - Milwaukee
  - (110)0151  4:44 2004
- A is for Action
  - Ina Robot
  - (107)0769  2:12 2004
- A Lesson In Longing
  - Somehow Hollow
  - (110)0574  2:08 2004
- A Little Too Much
  - Travis Abercrombie
  - (107)0392  2:57 2004
- A Million and One Thin
  - Time Machine
  - (101)0157  3:39
- Time Authority
  - Zero
  - (110)0060  3:52 2004
- A Modern Way of Letting
  - Idlewild
  - (108)0054  2:21 2004
- A NorthWest Passage
  - International Noise
  - Co
  - (110)0028  3:51 2004
- A Passage In Time
  - Authority Zero
  - (110)0429  2:08 2004
- A Question Mark
  - Elliott Smith
  - (107)0360  2:30
- A Runner’s Self-Portrait
  - Eastern Youth
  - (110)0181  4:31 2004
- A Trophy Mule in Part
  - Guided By Voices
  - (110)00429  2:08 2004
- A Walk
  - Bad Religion
  - (110)0132  2:09 2004
- Abbot & Costello
  - (103)0515  4:20 2004
- Abbot & Costello
  - (109)9999  4:15 2004
- Aboard The Ark
  - Apes, The
  - (110)0177  4:17 2004
- About A Girl
  - Nirvana
  - (107)0110  3:03 2004
- Acid Raindrops
  - People Under the Stairs
  - (101)0042  4:38 2003
- Acquiescence
  - Oasis
  - (107)0171  4:23 2004
- Action Happening
  - Cat On Form
  - (110)0441  2:42 2004
- Actual Proof
  - Herbie Hancock
  - (103)0425  8:15
- Add Mission
  - Apex Theory
  - (107)0092  3:31 2004
- Addicted
  - Simple Plan
  - (107)5021  3:50 2004
- Aenima
  - Tool
  - (108)5033  6:33 2004
- Aeroplane
  - Red Hot Chili Peppers
  - (107)0143  4:06 2004
Automagically Do Most Of This With Core IMPACT
Customize Core IMPACT

- A little Python and you’re on your way
- I started simple: deploy a flag in a capture the flag hacking challenge
- Drag and drop FTW!
- IMPACT also supports:
  - Grabbing frame from webcam
  - Recording audio
  - Keystroke logger
  - Remote packet sniffer
Phases

- Phase I - Target identification
- Phase II – Detect OS & Services
- Phase III – Identify Vulnerabilities
- Phase IV – Exploitation
- Phase V – Post-Exploitation
- **Phase VI - Reporting**
Reporting – A Picture Speaks…

Originally Titled “Vista Relief”
Reporting Tips

• Use the output from your tools wisely
  – Grab “Resources” for vulnerability from Nessus/Core to save time

• Automate as much as possible
  – Export Nessus to NBE, use Bash/Perl
  – Export Core to CSV? = Wish List!
Reporting Tips (2)

• Use screenshots & videos
  – Use screenshots that show risk, be selective
• Be concise and to the point
  – Include what you found, the effect it has on the organization, and how to fix it
• Include methodology
  – This allows customer/end user to re-test and reproduce results
• More info on reporting in:
  – “SEC561 Network Penetration Testing: Maximizing the Effectiveness of Reports, Exploits, and Command Shells”
Lessons Learned

• Exploitation is an important part of your testing to reduce false positives and provide integrity
• Remote exploits come in many forms, such as default passwords and open file shares
• Perform post-exploitation such as capturing screen, video, audio, keystrokes, and network traffic
• Report should contain what you found, the effect on the organization, and how to fix it
/* End */

- Forum discussion for this presentation: http://forum.pauldotcom.com
- Weekly podcast and more at http://pauldotcom.com

paul@pauldotcom.com