When the Tables Turn
Agenda

- Thinking about the concept
- Introduction
- Types of defensive technology
- Raising the bar
- Typical assessment methodology
- Attacks
- Examples
- Conclusion
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)
– Banners
– Forward & reverse DNS entries
– Error codes, messages
– Web pages

Used in the tool/scanner itself
Used in rendering of data, databases
Used in secondary scanners, reporters
Examples

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

```
[root@womwom dnsjava-1.6.2]# java jnamed jnamed.conf
jnamed: listening on 0.0.0.0#53
jnamed: running

$ 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
102.67.30.196.in-addr.arpa. 86400 IN PTR mh.sensepost.com
```
Examples

Network level:

Avoiding

   Firewall

Noise:

   honeyd & transparent reverse proxies
   - Random IPs alive
   - Random ports open
   - Traceroute interception/misdirection
   - Fake network broadcast addresses

Stopping:

   ?

Killing:

   nmap with banner display??
Examples

Network level:

Tools:

Ping sweeps / vitality checkers
Port scanners
nmap, paketto/pulse, superscan, visualroute, some custom scripts, etc.

etc.
Examples

Network level:

Tools:
- Ping sweeps / vitality checkers
- Port scanners
  - nmap, paketto/pulse, superscan, visualroute, some custom scripts, etc.

```perl
!/bin/perl

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


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;
```
017 fwd 127.0.0.1,8888 tcp from any to 196.30.67.126 80
018 fwd 127.0.0.1,7777 tcp from any to 196.30.67.66 80
019 fwd 127.0.0.1,2121 tcp from any to 196.30.67.66 21
021 fwd 127.0.0.1,1 icmp from any to 196.30.67.104
022 fwd 127.0.0.1,1 icmp from any to 196.30.67.124
023 fwd 127.0.0.1,1 icmp from any to 196.30.67.102
024 fwd 127.0.0.1,1 icmp from any to 196.30.67.85
025 fwd 127.0.0.1,1 icmp from any to 196.30.67.113
026 fwd 127.0.0.1,8080 tcp from any to 196.30.67.68 80
027 fwd 127.0.0.1,8080 tcp from any to 196.30.67.119 80
028 fwd 127.0.0.1,8080 tcp from any to 196.30.67.79 80
029 fwd 127.0.0.1,8080 tcp from any to 196.30.67.90 80
030 fwd 127.0.0.1,8080 tcp from any to 196.30.67.89 80
031 fwd 127.0.0.1,8080 tcp from any to 196.30.67.69 80
032 fwd 127.0.0.1,8080 tcp from any to 196.30.67.95 80
033 fwd 127.0.0.1,2121 tcp from any to 196.30.67.89 21
034 fwd 127.0.0.1,2121 tcp from any to 196.30.67.113 21
035 fwd 127.0.0.1,2121 tcp from any to 196.30.67.74 21
036 fwd 127.0.0.1,7777 tcp from any to 196.30.67.98 2049
037 fwd 127.0.0.1,7777 tcp from any to 196.30.67.74 433
038 fwd 127.0.0.1,7777 tcp from any to 196.30.67.101 99
039 fwd 127.0.0.1,7777 tcp from any to 196.30.67.67 512
040 fwd 127.0.0.1,7777 tcp from any to 196.30.67.102 700
041 fwd 127.0.0.1,7777 tcp from any to 196.30.67.93 79
042 fwd 127.0.0.1,7777 tcp from any to 196.30.67.67 81
043 fwd 127.0.0.1,7777 tcp from any to 196.30.67.88 139
044 fwd 127.0.0.1,7777 tcp from any to 196.30.67.78 513
045 fwd 127.0.0.1,7777 tcp from any to 196.30.67.88
Examples

Network application level

Avoiding
- Patches, patches

Noise:
- Fake banners
- Combined banners
- NASL (reverse) interpreter

Stopping:
- Tar pits

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, Sara & friends?
Commercial: ISS, Retina, Typhon, Foundscan, Qualys, Cisco
Examples

Application level & (web server assessment)

Avoiding

Application level firewall

Noise:
- On IPs not in use:
  - Random 404, 500, 302, 200 responses
  - Not enough to latch “friendly 404”, or intercept 404 checking
- Within the application
  - Bogus forms, fields
  - Pages with “ODBC ….”

Stopping:
  - Spider traps, Flash, Human detectors

Killing:
- “You are an idiot!”
- Bait files.. Admintool.exe and friends in /files,/admin etc.
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
Examples

Armpit1

Incoming connection

Valid cookie?

Valid request string?

Send valid cookie and redirect

Back to client

Build and send Flash

Relay connection

Back to client
### 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-msdownload, application/octet-stream, <em>/</em></td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-us</td>
</tr>
<tr>
<td>Cookie</td>
<td>pof=waysecret</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)</td>
</tr>
<tr>
<td>Host</td>
<td>196.30.67.30</td>
</tr>
<tr>
<td>Connection</td>
<td>close</td>
</tr>
</tbody>
</table>
Examples

Armpit2

With

Send valid cookie and redirect

Valid request string?

no

direct

no

Send valid cookie and redirect

Valid request string?

yes

Send valid cookie and redirect

Evil request?

yes

BlackList Cookie & close connection

no

Stop

Back to client

damaged connection

no

Back to client

Back to client
Combining with IPS

You are naughty
I will blacklist your Cookie

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.
• IPS can easily switch on “armpits”
• It’s a whole new ballgame…
QUESTIONS??
COMMENTS??
FLAMES??

When the Tables Turn

BLACKHAT
AMSTERDAM
2004

sensepost