BLACKHAT AMSTERDAM 2004

REVENGE IS A DISH BEST SERVED COLD

When the Tables Turn

sensepost

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; “lets 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…

2004 BLACKHAT AMSTERDAM

sensepost

Examples

Untitled - Notepad

File Edit Format View Help

```
[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|ls.
200.67.30.196.in-addr.arpa. 86400 IN PTR s.<B>test</b>.sensepost.com.
10.67.30.196.in-addr.arpa.  86400 IN PTR rexacop.sensepost.com.
102.67.30.196.in-addr.arpa. 86400 IN PTR mh.sensepost.com`|ls`.
```

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??

sensepost

Examples

Network level:

Tools:

Ping sweeps / vitality checkers

Port scanners

nmap, paketto/pulse, superscan, visualroute, some custom scripts, etc. etc.

e Edit Format View Help

```
!/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","
3","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;
```

ntitled - Notepad

Edit Format View Help

```
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

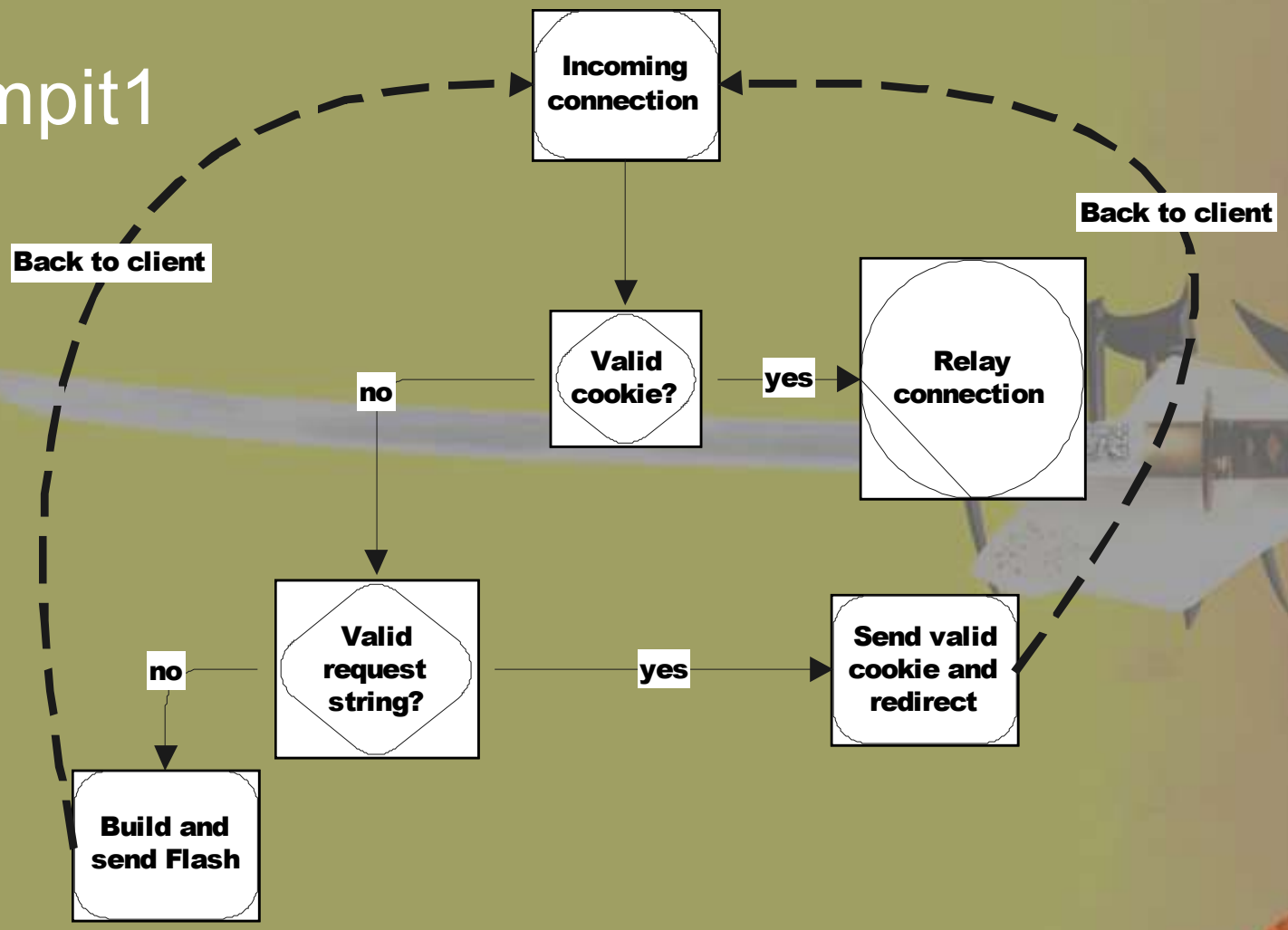
Tools:

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



2004 BLACKHAT AMSTERDAM
sensepost

@stake WebProxy - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://webproxy/ Go Links

Google Search Web 220 blocked

Admin | RequestIntercept | RequestFuzzer | RegexReplacement | Quash | FileWriter | RequestCache | RequestEditor | Utilities

@stake WebProxy 1.0

RequestEditor Plugin

Requested Urls
http://196.30.67.30/
http://196.30.67.30/p=12345678999999
http://196.30.67.30/reroute.swf
http://196.30.67.30/

@stake WebProxy -

File Edit View Fav

Back

Address http://webpr

Google

Admin Reques

Request Method	
Request Resource	
Request Version	

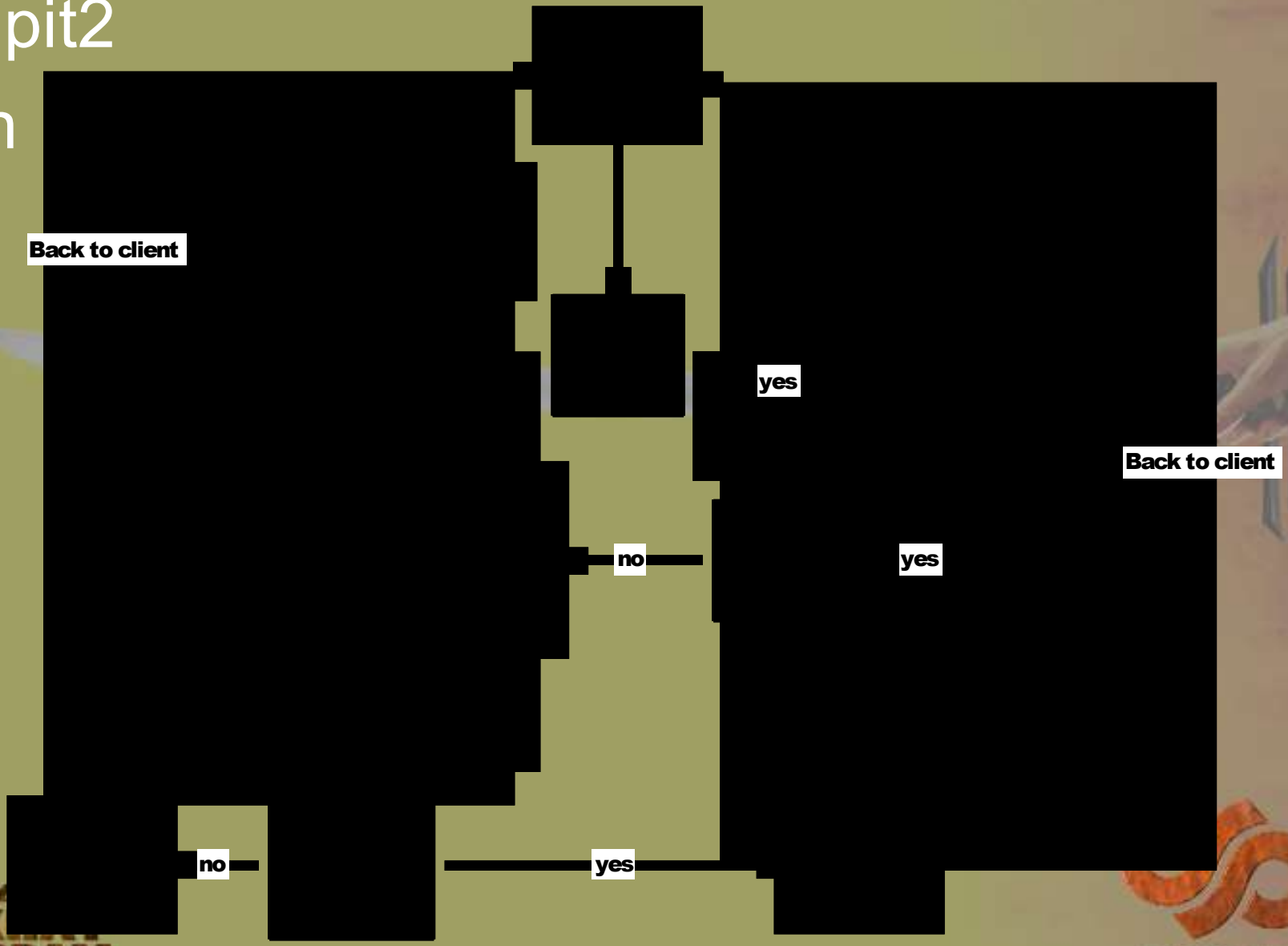
Header Parameters

Name	Value	Delete
Accept	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-pov	☐
Accept-Language	en-us	☐
Cookie	poef=waysecret	☐
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	☐
Host	196.30.67.30	☐
Connection	close	☐

Examples

Armpit2

With



2004 BLACK HAT AMSTERDAM
sensepost

Combining with IPS

http://196.30.67.30/show.php?p=20'exec master..xp_cmdshell 'cls'-- - Microsoft Intern...

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://196.30.67.30/show.php?p=20'exec%20master..xp_cmdshell%20'cls'-- Go Links

Google teleportpro download Search Web 220 blocked

You are naughty

I will blacklist your Cookie

http://196.30.67.30/show.php?p=20'exec%20master..xp_cmdshell%20'cls'--

Done Internet

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??