



Economies of Scale in Hacking

Dave Aitel

Immunity

Ekoparty, 2008 (Argentina)

Demand Side/Supply Side Economies of Scale

- Networked increase in value
- High barrier of entry
- Cheaper as you get bigger



Applying this to hacking

The best offense is a good offense

Your source code wants to be free

The 10.0.0.0 and IPv6 problems

Networked reverse engineering toolkits

Attack frameworks

XSS vs Heap Overflows



Ignore the network effects to your own peril

- Case Studies:
 - AV
 - IDS
 - Static Analysis
- Questions to ask:
 - What is growing exponentially?
 - How did the technology handle that?

The Twitter Effect

- To Twitter: (verb)
to fail under
exponential
growth



The image is a screenshot of the Twitter website's homepage. At the top left, the word "twitter" is written in its signature blue, lowercase font. Below this, the heading "What is Twitter?" is displayed in bold black text. To the right of the heading are three buttons: "What?" (solid), "Why?" (dashed), and "How?" (dashed). Below the heading is a large graphic featuring a yellow bird perched on a dark brown branch that curves into a series of blue and white swirls. To the right of the bird graphic is a vertical stack of three tweet snippets. The top snippet shows a profile picture and text: "Ey Waited all morning for PC&E, who didn't without power or internet let me get some over, back at office. 2 minutes ago from txt". The middle snippet shows a profile picture and text: "Maggie Just landed in LA. 2 minutes ago". The bottom snippet shows a profile picture and text: "mollydotcom wishes she could sleep recovering from trauma. 2 days of dr web...". At the bottom of the page, a green button with white text reads "Get Started—Join!".

Anti-Virus

Allchin Suggests Vista Won't Need Antivirus

By [Scott M. Fulton, III](#), BetaNews
November 9, 2006, 4:26 PM

During a telephone conference with reporters yesterday, outgoing Microsoft co-president Jim Allchin, while touting the new security features of Windows Vista, which was [released to manufacturing yesterday](#), told a reporter that the system's new lockdown features are so capable and thorough that he was comfortable with his own seven-year-old son using Vista without antivirus software installed.

Allchin's statement that Vista would be secure without security features he said, his pe



F-Secure: Malware Doubled in 2007
December 06, 2007 | by [Geoff Duncan](#)

F-SECURE

Computer security firm F-Secure was tracking about 250,000 malware signatures at the beginning of 2007: now, they're tracking about 500,000.

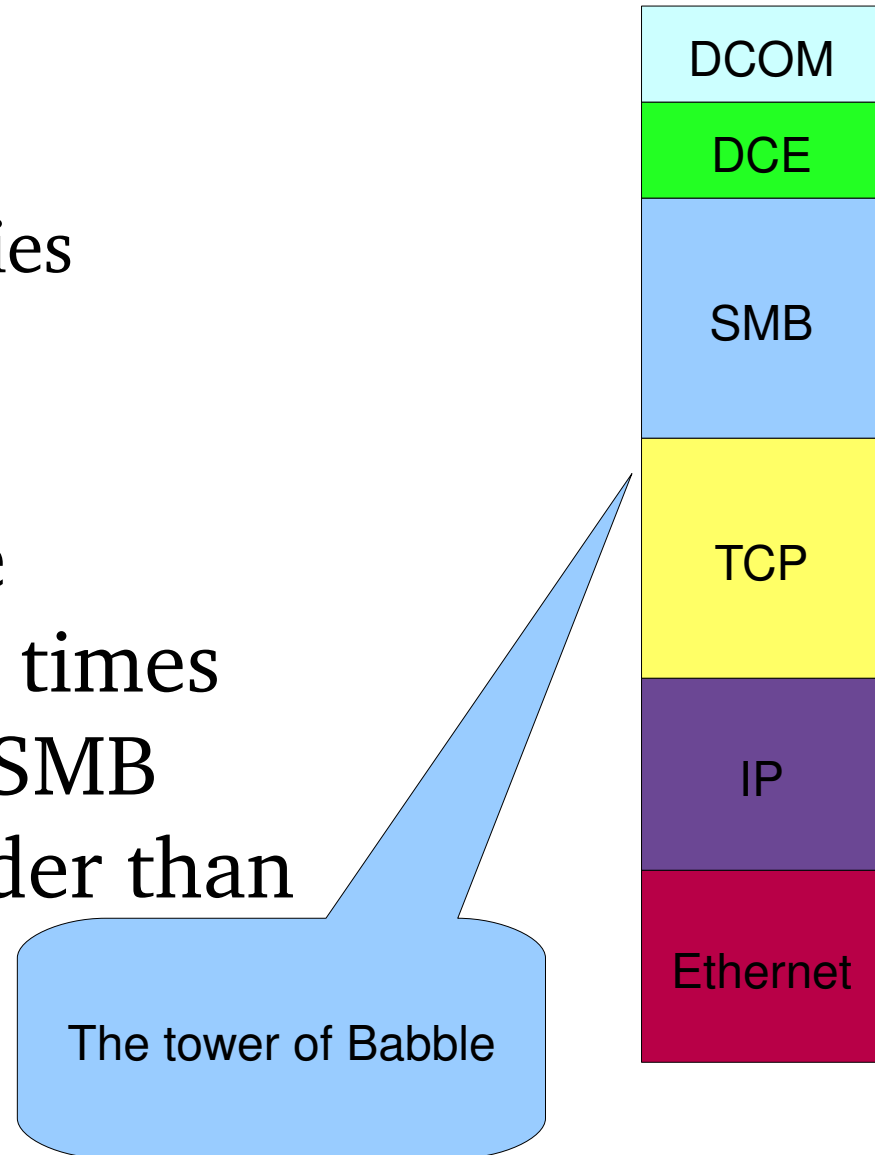
Not a good sign



6 hours to defeat 10 AV's

IDS: What grows exponentially?

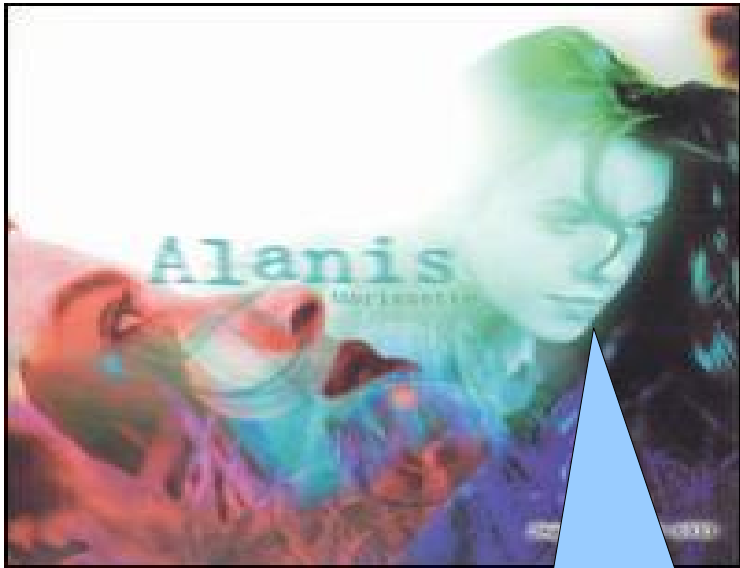
- Targets
 - And hence vulnerabilities
- Protocols
 - Protocol complexity
- IDS/IPS failed because decoding DCOM is ten times harder than decoding SMB which is ten times harder than decoding IP



Static Analysis: Checklists are not the answer

- NIST Static Analysis survey
 - 6 target programs (Java/C)
 - Lots of products and services
 - Extremely high false positive rate
 - Over 1 man year to sort through 47000 warnings
 - Guess how many 0day they found!?

Best of the 90's



Security Problem?

Sniff For It

Scan for it

Demand Side Economies of Scale: Offense == More Offense

The best offense is a
good offense



The best password cracker in the world

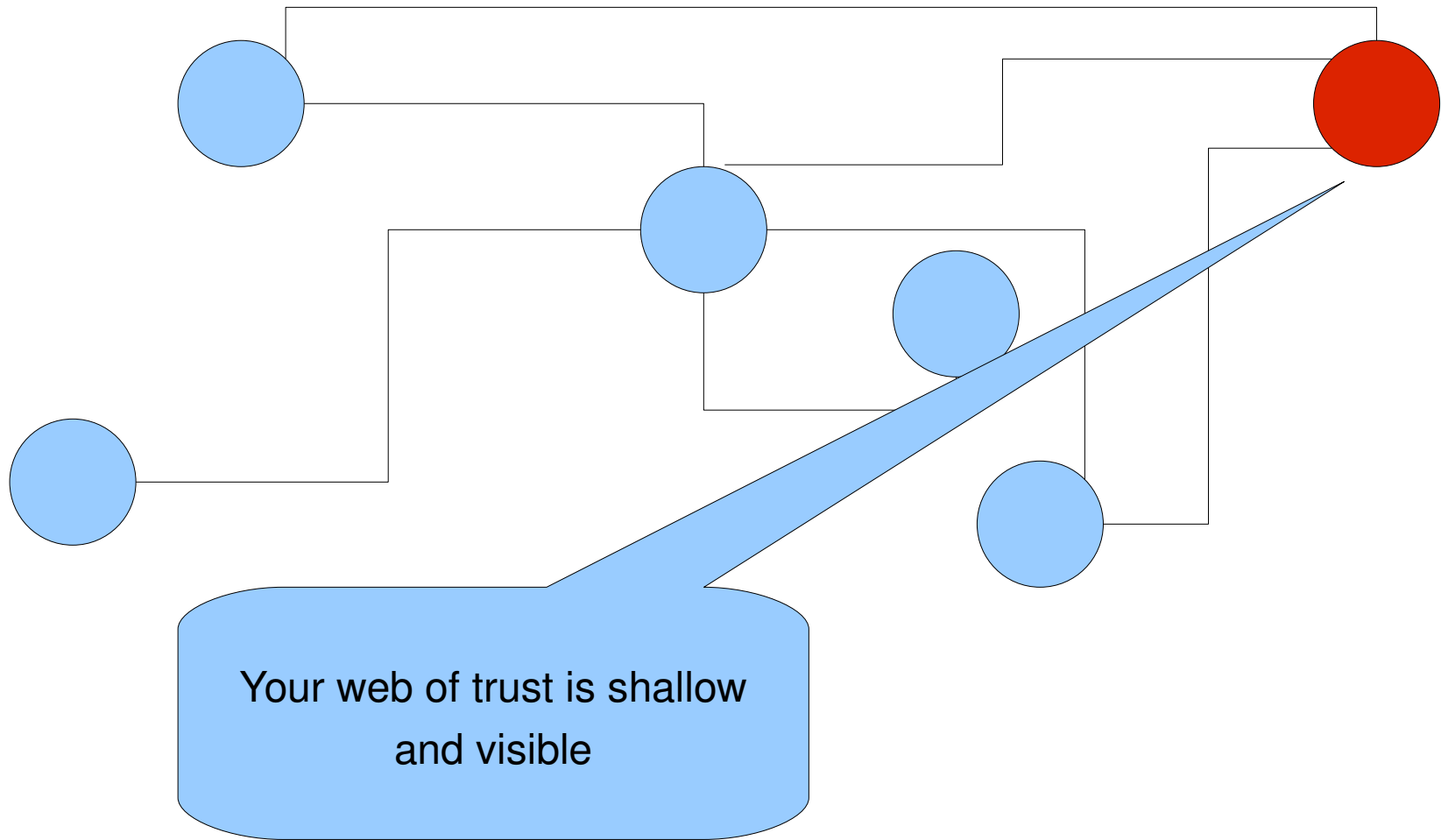
?

The best password cracker in the world

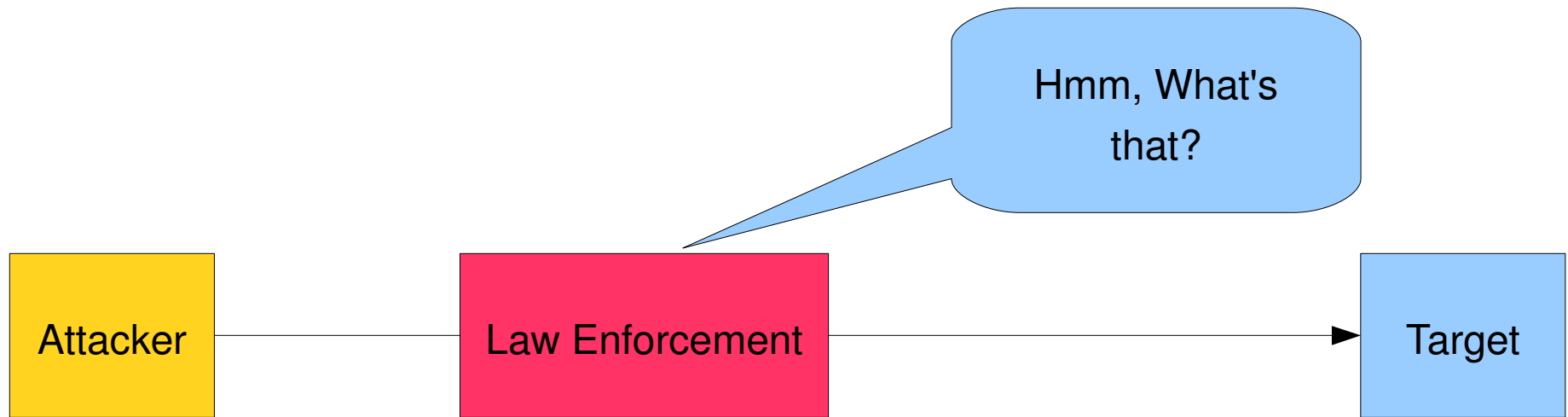
```
grep targetname passwords.txt
```

Chances are I
already have your
password

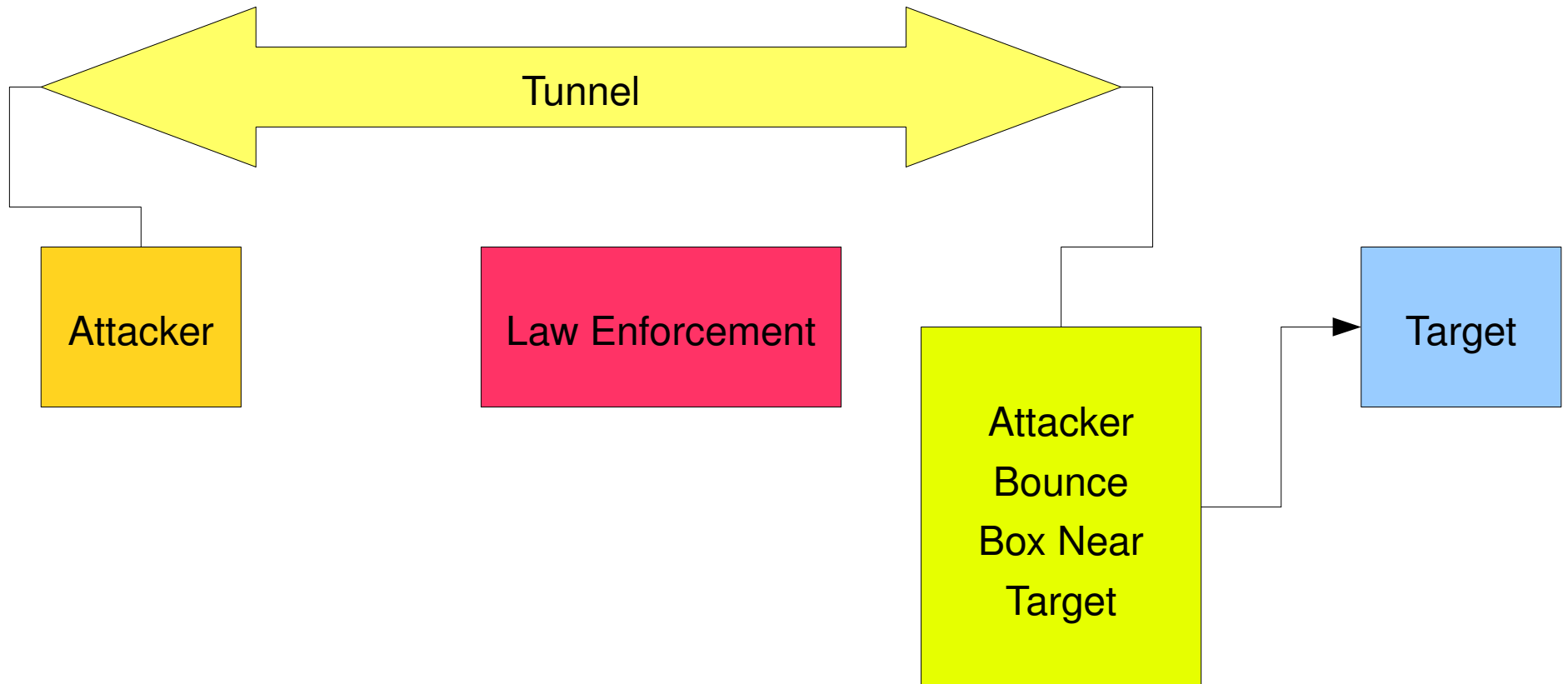
To a hacker who is everywhere...



Poor Attacker



Rich Attacker



Trust the Source

Your source code wants
to be free



“Damage” is strategic, not monetary

Re: Kevin Mitnick

Dear Kathleen:

Congratulations on the arrest of Kevin Mitnick. Pursuant to your request, I asked our Cellular group to assess the damages caused to Fujitsu Network Transmission Systems, Inc. ("FNTS") by Mitnick's theft of the source code for the PCX telephone. The information provided to me is as follows:

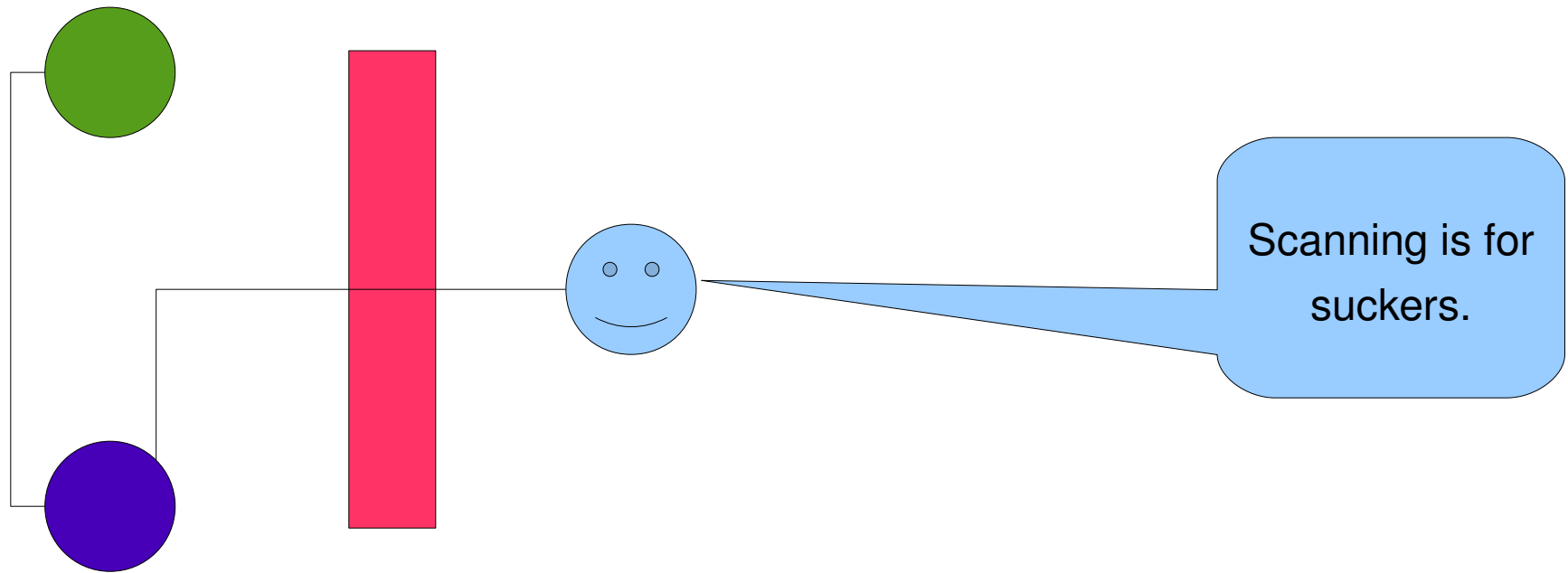
Software development expenses...	\$1,100,000.00
Research & development expenses..	1,000,000.00
Total...	\$2,100,000.00

Networks, plural.



The 10.0.0.0 and IPv6 problems

10.0.0.owned



OS Detection

- Knowing a host is Windows 2000 is great for scanner reports
- To get beyond the scanner reports we need to think beyond “OS” to a concept of “is this vulnerable” and “will this be vulnerable”.
 - Automated statistical techniques can do this on a large scale

GIT + ASM = GITASM?

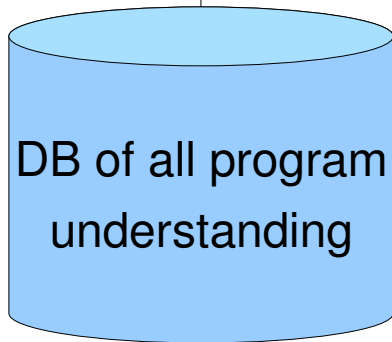


Networked reverse
engineering toolkits

There's no I in hacking.

```

PUSH EBP
MOV EBP,ESP
SUB ESP,238                stack vars total - size 568 bytes
PUSH EBX
PUSH ESI
PUSH EDI
F LEA EDI,DWORD PTR SS:[EBP-238]    stackvar_2 - size: 64 bytes
MOV ECX,8E
MOV EAX,CCCCCCCC
REP STOS DWORD PTR ES:[EDI]
PUSH 1F4
PUSH 0
F LEA EAX,DWORD PTR SS:[EBP-1F8]    stackvar_1 - size: 500 bytes
PUSH EAX
CALL NOP1._memset
ADD ESP,0C
F LEA ECX,DWORD PTR SS:[EBP-1F8]    stackvar_1 - size: 500 bytes
MOV DWORD PTR SS:[EBP-4],ECX
MOV EDX,DWORD PTR SS:[EBP+10]
PUSH EDX
MOV EAX,DWORD PTR SS:[EBP+C]
PUSH EAX
PUSH NOP1.0042101C
F LEA ECX,DWORD PTR SS:[EBP-1F8]
PUSH ECX
CALL NOP1._sprintf
sprintf -> POSSIBLE SPRINTF STACK OVERFLOW
    
```



BinNavi - 0 Flowgraph - Address: 00402A5F name: sub_402A5F

```

00402B1C mov     edx,ss[ebp+0x10]
00402B20 push  edx
00402B22 call  cs:[00402B20]
00402B28 mov     ss[ebp+0x10],eax
    
```

```

00402B2B cmp     ss[ebp+0x10],0
00402B2E js      byte cs:[00402B2B]
    
```

```

00402B31 mov     eax,ss[ebp+0x10]
00402B34 push  eax
00402B35 call  cs:[00402B35]
00402B38 add     esp,4
00402B3D mov     ecx,ss[ebp+0x10]
00402B40 mov     edx,ds[ecx]
00402B42 or      ecx,eax
00402B44 mov     eax,ss[ebp+0x10]
00402B47 mov     ds[eax],edx
00402B49 push  ecx
00402B4B mov     ecx,ss[ebp+0x10]
00402B4E push  ecx
00402B51 add     esp,-0x4
00402B54 add     esp,4
00402B57 mov     ss[ebp+0x10],eax
00402B5A cmp     ss[ebp+0x10],0
00402B5E js      byte cs:[00402B5E]
    
```

```

00402B60 mov     edx,ss[ebp+0x10]
00402B63 add     edx,1
00402B66 push  edx
00402B68 call  cs:[00402B68]
00402B6C add     esp,4
00402B6E mov     ecx,ss[ebp+0x10]
    
```

```

00402B80 mov     eax,ss[ebp+0x10]
00402B83 mov     eax,ss[ebp+0x10]
00402B86 call  cs:[00402B86]
    
```

Output

```

Loop found, blocks are:
[00402B60, 00402B7B, 00402B82, 00402B81]
    
```

Applying this to hacking



Attack
frameworks

Know Your Customer

- “iTunes” for Exploits
- “Facebook” for trojans
- Customer Relationship Management for targets

This is not your father's heap



XSS vs Heap
Overflows

The Bazaar

- Good offensive security research is being driven underground
 - It's too expensive to give away!
 - Not just a “Vulnerability Marketplace”:
 - Audit technologies
 - Bug classes
 - Exploit techniques



Show me the MONEY!

Why are memory corruption bugs so expensive

- **Heap/Stack cookies (/gS)**
- **SafeSEH**
- **ASLR**
- **DEP/NX/W ^ X/PAX**
- **Process Isolation**
- **System call ACLs**
- **Automated code review programs**
- **Managed languages**

Security made the news

- Security built into development lifecycles
 - And compiler tools
- Security responses driving vendor differentiation
- Security being built into platforms

A gathering storm

- “But this doesn't affect me - I write web applications in Ruby on Rails”
- “There hasn't been a real remote overflow in IIS since version 5”
- “What part of **managed** language don't you understand?”



This is all true!

\$- > \$\$\$

- Vulnerability research is so expensive it cannot be funded out of your marketing budget anymore
- Not only are bugs expensive but the techniques for reliably exploiting bugs becomes expensive
 - You no longer know if you are really at risk!

The market is reacting

- The memory corruption problem is “solved”
- The worm problem is “solved”
 - Hence, the slow takeup of IPS – it's just not worth the pain!
- Microsoft Exploitability Index
 - Q: What are you going to do when for months on end everything is “pretty much not exploitable”
 - A: Stop patching
 - A: Stop investing in security

Exploit 7 Impossible Bugs Before Breakfast



Things you can do at large scale

- Defeat Secure Development Lifecycles
- Attain a significant advantage by combining different levels of information

Attack the next big mistake

- C/C++
 - Memory corruption
- Ruby on Rails, Java, C#, Python, etc.
 - No buffer overflows (we're MANAGED)
 - Threading!

The Conclusion

Hacking has a strong trend towards natural monopoly!