Penetration Testing Lessons Learned

IMMUNITY

Security Research

Who am I?

- CTO at Immunity, Inc.
- Privately held information security company
  - Consulting
  - Training
  - Specialized Security Products
    - CANVAS
    - SILICA
- Based in Miami Beach

Remote Shells Can Happen To Anyone

- Vertical: Manufacturing
- Scope: 1-week Web Assessment of a single employee admission process application (semi-blind)
- Result: J2EE based application was installed on Windows – was able to upload “trojan.jsp “ (with trailing space) and then browse to it.
- Mitigation: Customer removed upload functionality entirely, and planned a move to Linux

3rd Party Software = Fun

- Vertical: Financial
- Scope: 2 week internal assessment of large web application assessment and entire environment
- Was previously assessed by Immunity
- Has rather advanced custom IDS based on SQL Server Queries being sniffed and checked for anomalies

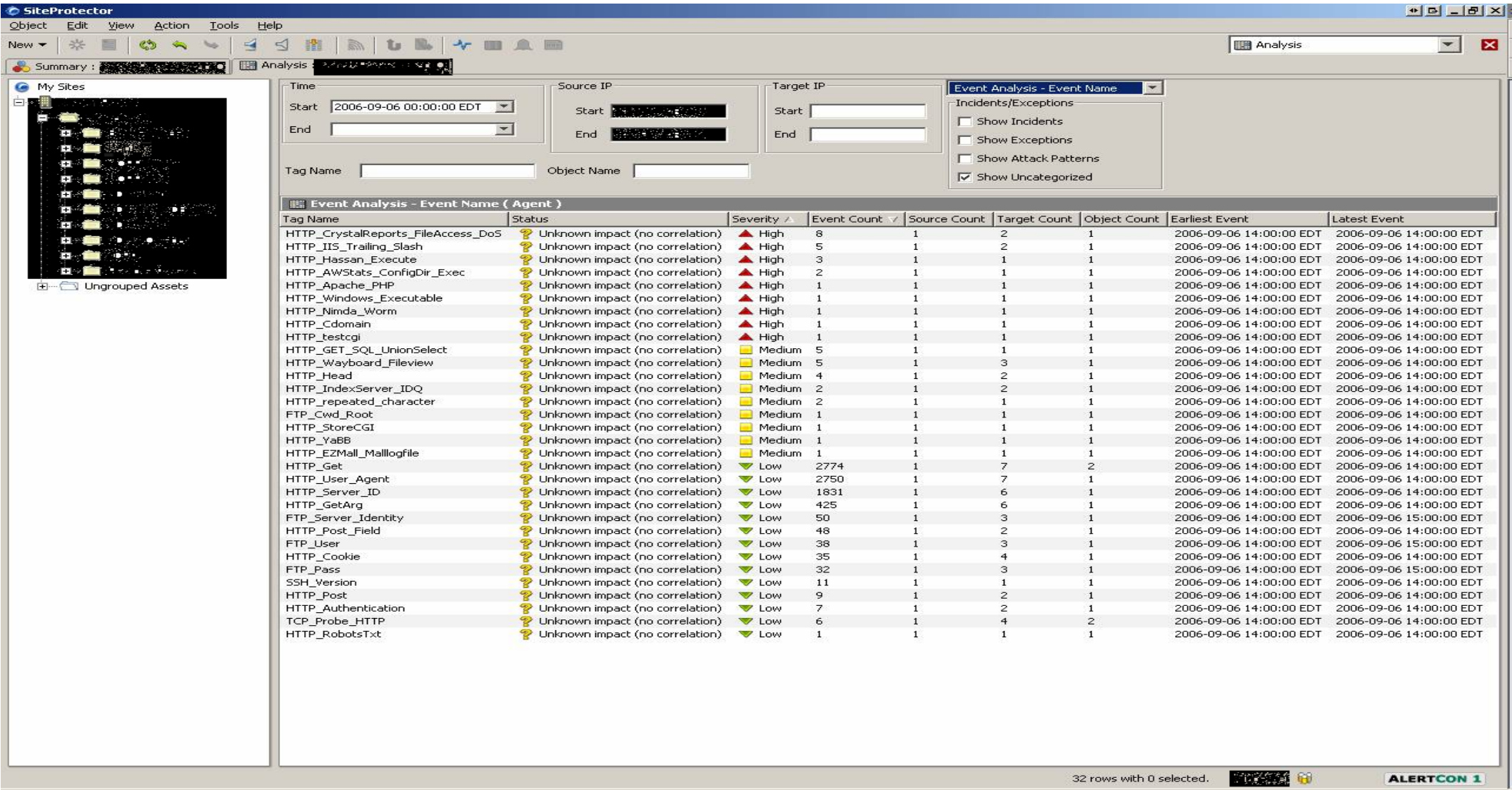
Serv-Who?

- Serv-U
  - old “vulnerable” version of 6.1.0.1
  - No known advisory or exploit
  - Immunity did fast binary assessment and attempted fuzzing, but no luck
- Bob's Charting Server
  - Found several vulnerabilities, but did not get a shell from them

Architecture is hard

- DB Tiers tied together
  - Null SA passwords found
- COM+ required massive firewall ruleset holes
- No exfiltration filters
  - IE vulnerability went public during test

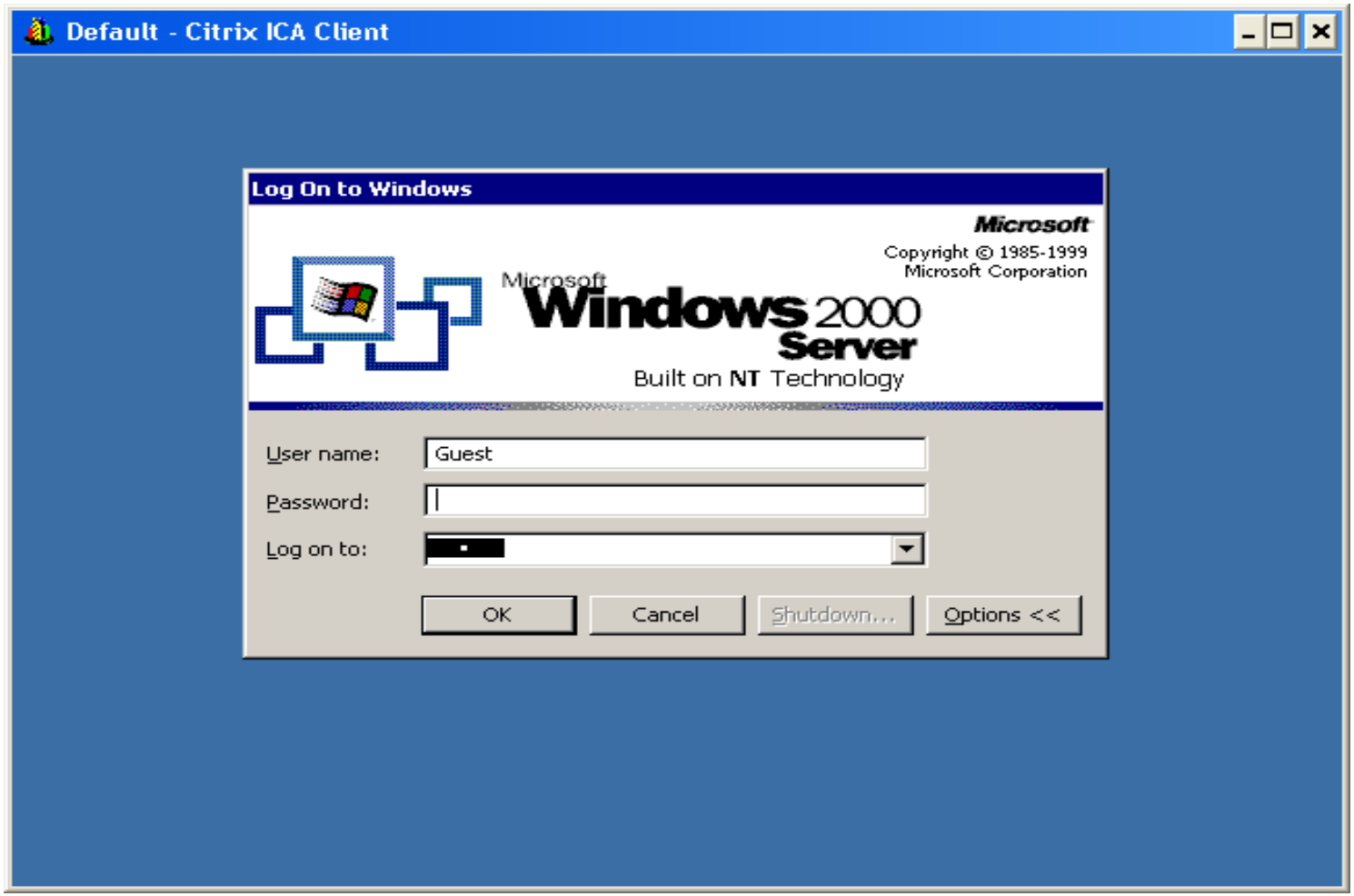
IDS Doesn't Work



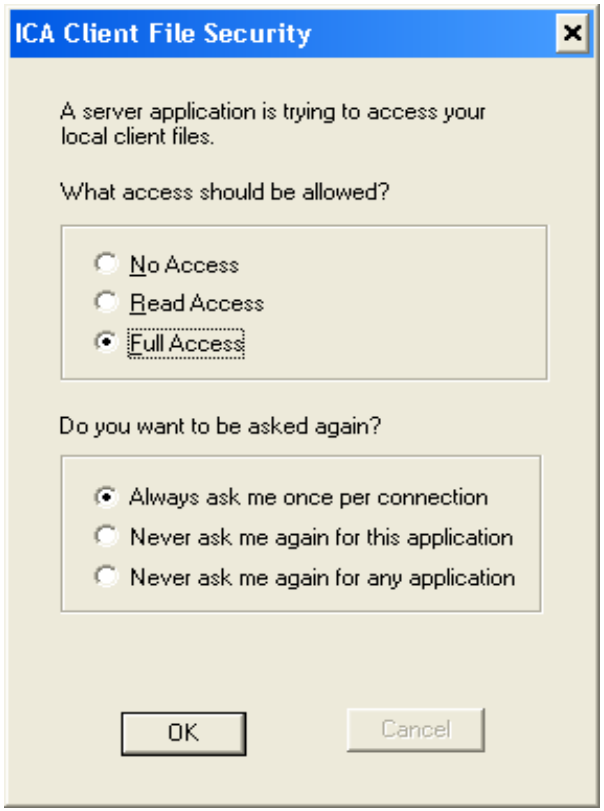
Remote Anonymous Ownership

- Vertical: Manufacturing
- Scope: Remote, anonymous penetration test of class C, open-source information gathering
  - mail servers
  - web servers
  - DNS servers
  - webmail
  - a customer portal
  - a Citrix server connection

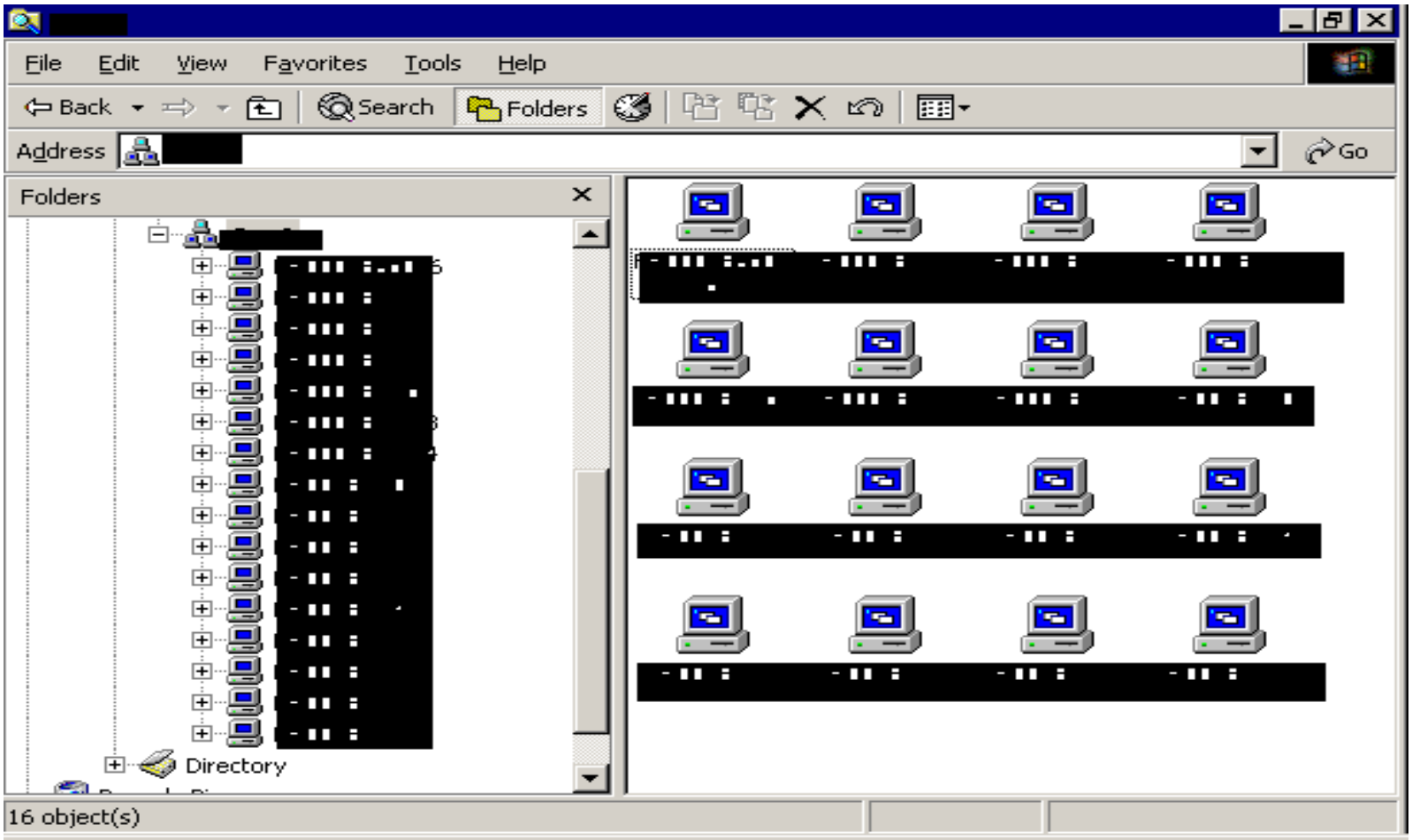
Remote access please!



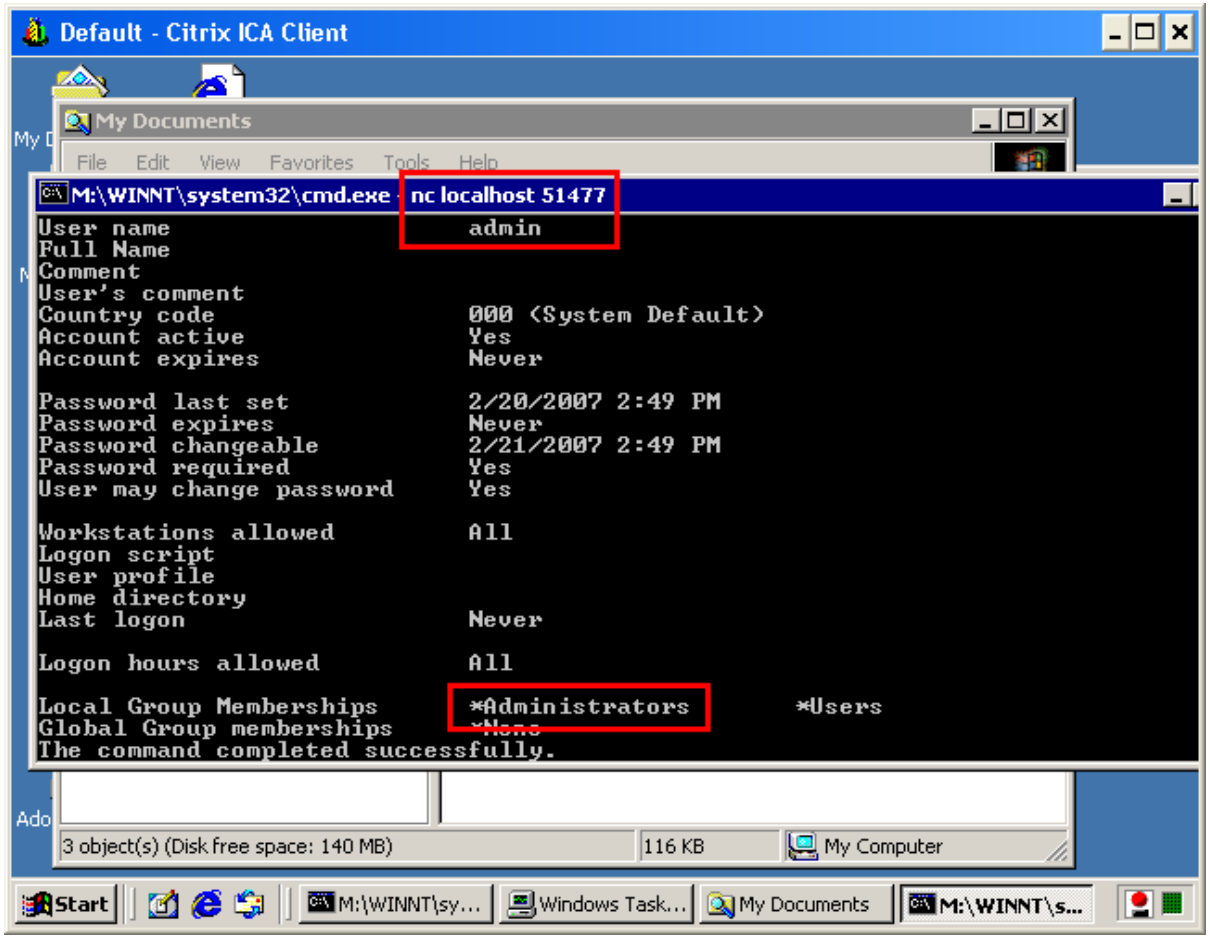
File sharing is nice too...



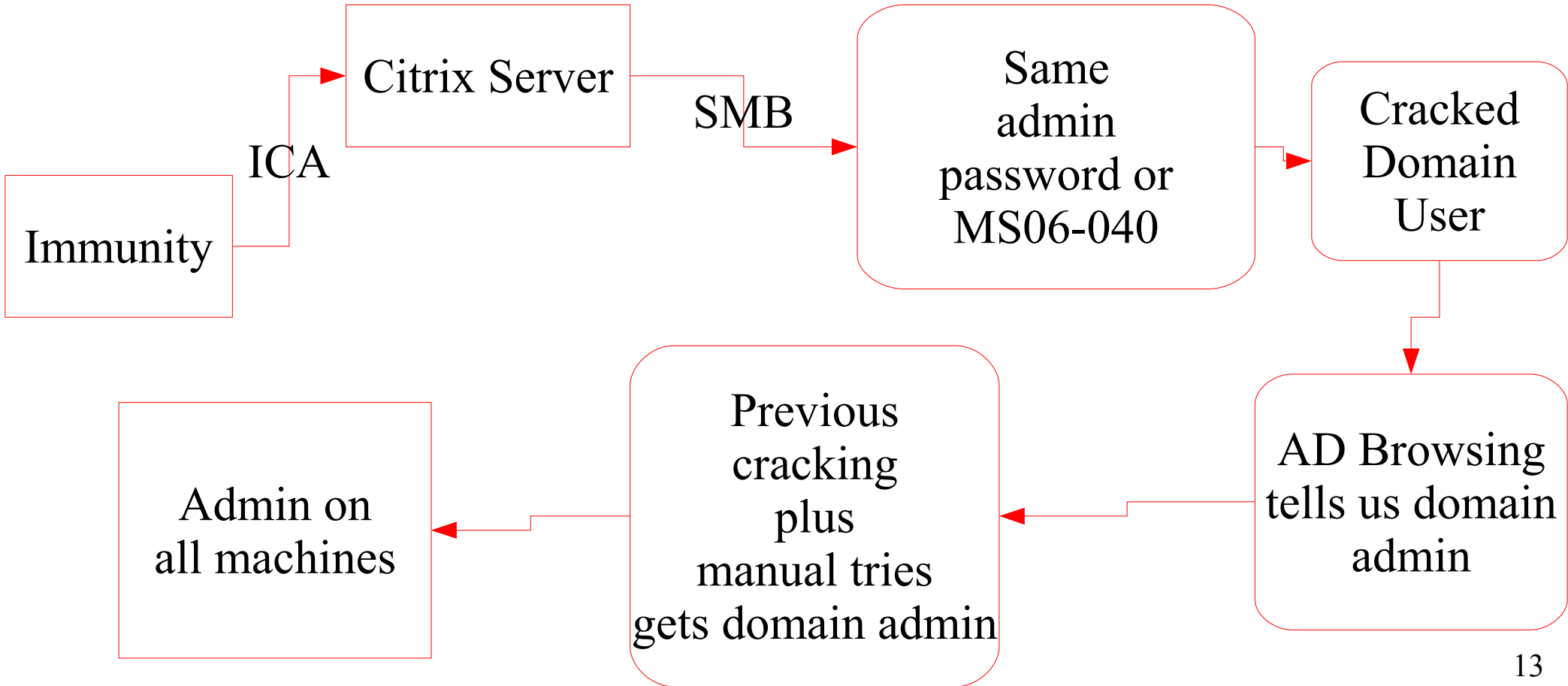
Lots of machines to see now



Being Admin is more fun (thanks Citrix Print Provider Overflow!)



This only looks easy...



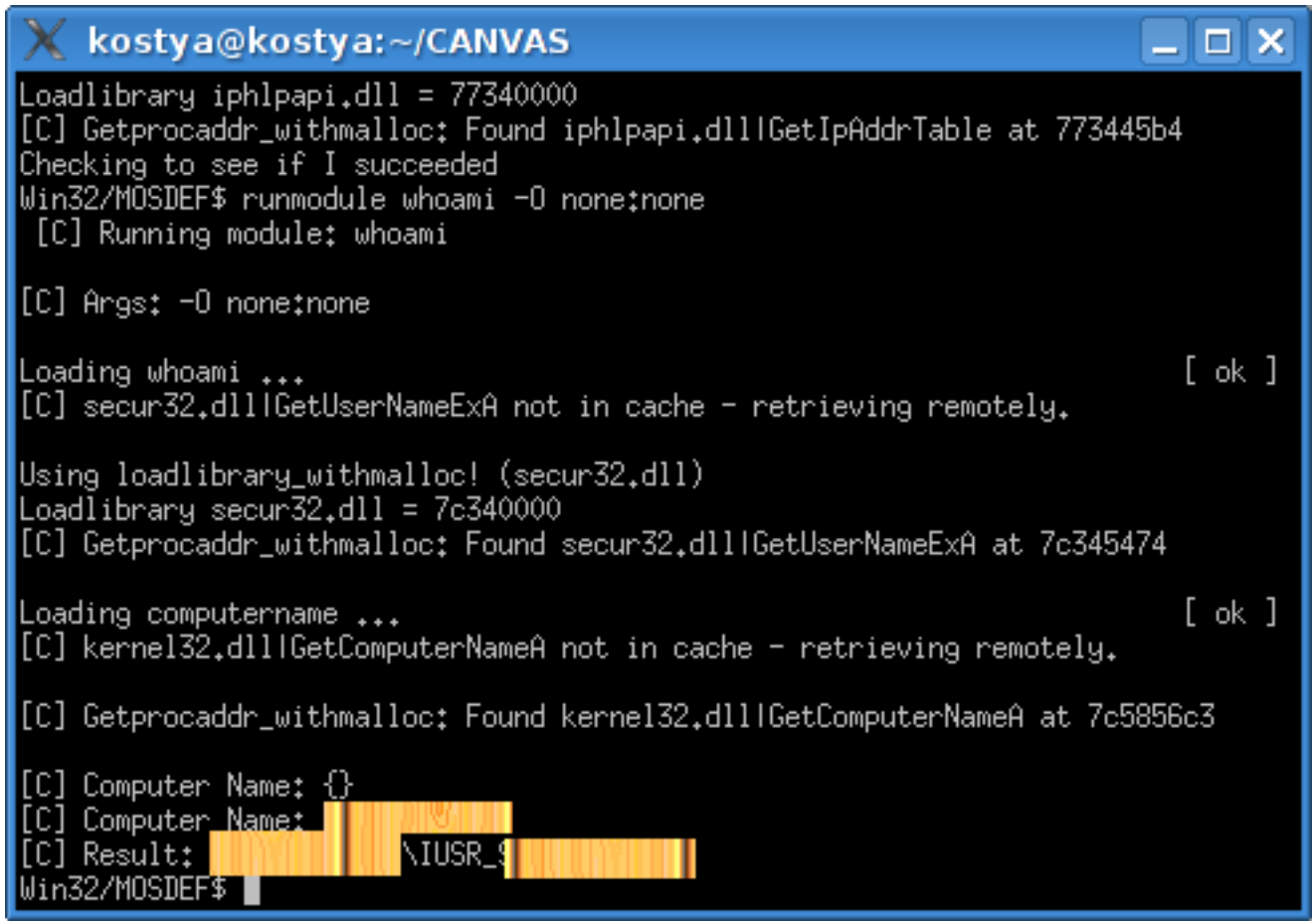
Open Source Information

- Places your employees go
  - Spoke – install a Browser Helper Object to export company information anyone?
  - FuckedCompany
  - Vault.com
  - Google/Yahoo groups

Not even 0day works every time

- Vertical: Manufacturing
- Scope: Assess custom website
- Result: Binary analysis of /scripts/bobip.dll finds heap overflow

0day to Remote MOSDEF Shell!



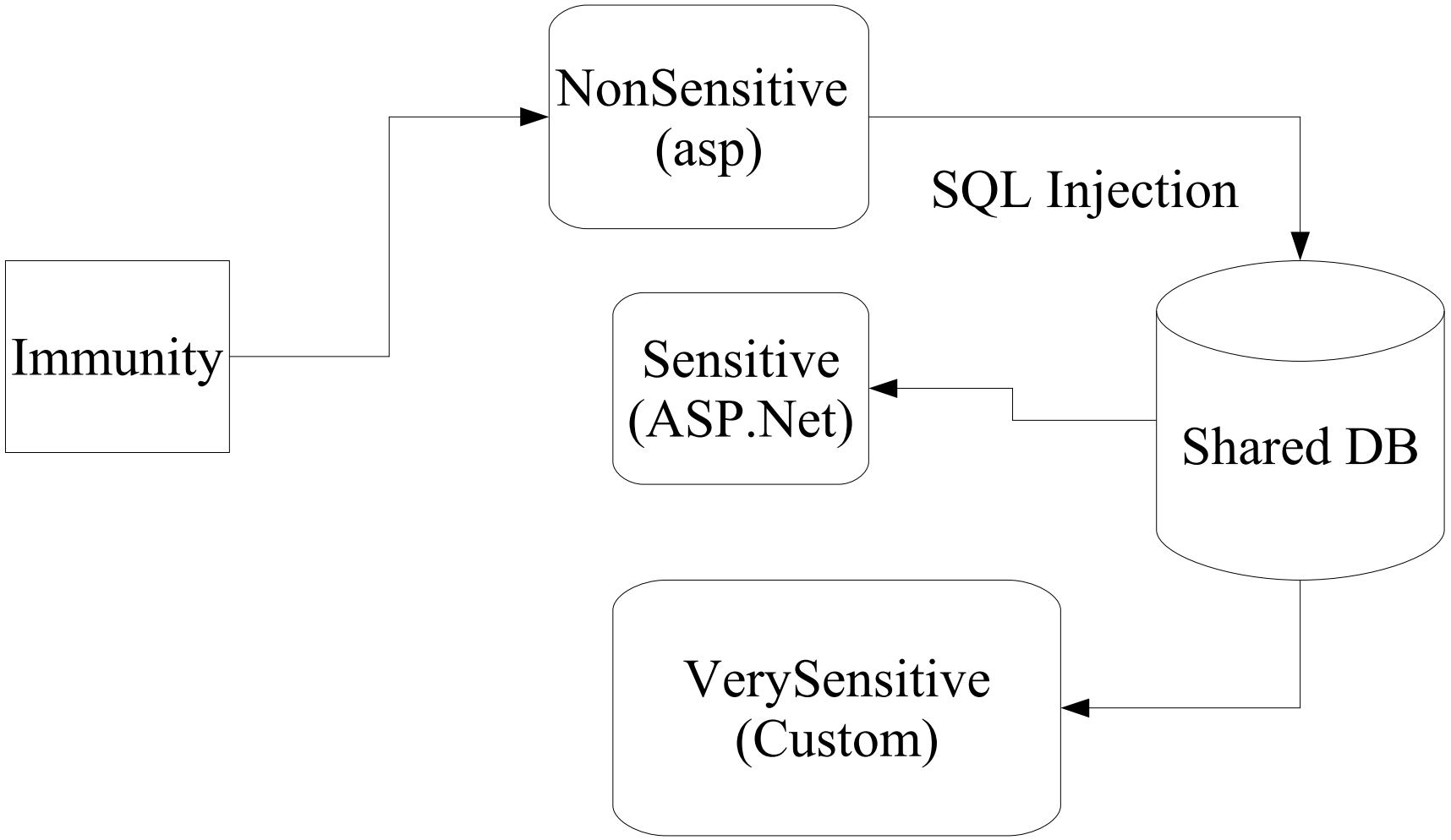
Sometimes a firewall will slow you down

- MOSDEF shell dies after a few minutes. Why?
  - Connection was getting a RST for no reason
  - Tried many variations on the shellcode, which seemed to improve things
  - But reaction of target was random – so what was the problem?
  - Post-game analysis indicates probable PIX firewall was closing our connection since we tunnelled over HTTP but did not look like HTTP

Quick hits under pressure

- Vertical: Financial
- Scope: several hour night assessment of 3 class C networks
- Result: Found SQL Injection, some cross site scripting. Exploited SQL Injection to dump database information, but was unable to get shell access. First ODBC error was found in three hours.

Architecture is a continuing problem!



Follow up is essential

- Scope: Same application, but on-site and informed
- Customer ran $25K automated web “penetration testing” tool as well
  - 100% false positives and 100% false negatives

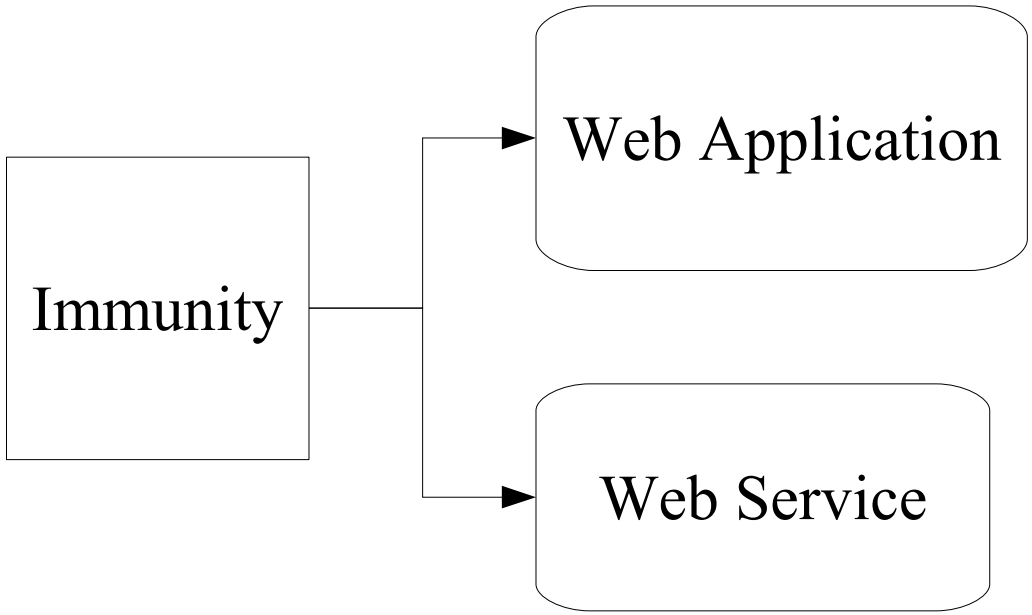
Results

- Cryptographic problem in cookie
  - Can replace usernames and become other people
- Remote File Include
  - Useful for turning a black-box test into a white-box test
- Overflows
- Oversight commission not amused

The latest technology is not the most secure

- Vertical: Manufacturing
- Scope: 1 week penetration test of web application
- Architecture: Modern Web 2.0 application built on IIS 6.0, Flash, and Adobe FLEX

Auth problems



- Nothing tied the authentication together!
- Web authentication also easily bypassed

Conclusions

- 0day vulnerabilities on third party components are a large part of penetration testing
- There's more to web application testing than Cross Site Scripting and SQL Injection
  - Automated scanners are not finding the problems
- A poorly designed architecture can make life a lot more fun for a hacker

Thank you for your time

Contact me at:

dave@immunityinc.com