

Penetration Testing Lessons Learned



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

KNOWING YOU'RE SECURE

IDS Doesn't Work

The screenshot displays the SiteProtector software interface. On the left is a tree view of 'My Sites' and 'Ungrouped Assets'. The main area is titled 'Event Analysis - Event Name (Agent)' and contains a table of security events. The table has columns for Tag Name, Status, Severity, Event Count, Source Count, Target Count, Object Count, Earliest Event, and Latest Event. The events listed include various HTTP and FTP actions, many with 'Unknown impact (no correlation)' and 'High' severity. The status column shows a yellow question mark icon for all events. The bottom right corner of the window shows '32 rows with 0 selected.' and the 'ALERTCON 1' logo.

Tag Name	Status	Severity	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
HTTP_CrystalReports_FileAccess_DoS	Unknown impact (no correlation)	High	8	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_IIS_Trailing_Slash	Unknown impact (no correlation)	High	5	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Hassan_Execute	Unknown impact (no correlation)	High	3	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_AWStats_ConfigDir_Exec	Unknown impact (no correlation)	High	2	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Apache_PHP	Unknown impact (no correlation)	High	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Windows_Executable	Unknown impact (no correlation)	High	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Nimda_Worm	Unknown impact (no correlation)	High	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Cdomain	Unknown impact (no correlation)	High	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_testcgi	Unknown impact (no correlation)	High	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_GET_SQL_UnionSelect	Unknown impact (no correlation)	Medium	5	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Wayboard_Fileview	Unknown impact (no correlation)	Medium	5	1	3	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Head	Unknown impact (no correlation)	Medium	4	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_IndexServer_IDQ	Unknown impact (no correlation)	Medium	2	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_repeated_character	Unknown impact (no correlation)	Medium	2	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
FTP_Cwd_Root	Unknown impact (no correlation)	Medium	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_StoreCGI	Unknown impact (no correlation)	Medium	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_YaBB	Unknown impact (no correlation)	Medium	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_EZMail_Mallogfile	Unknown impact (no correlation)	Medium	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Get	Unknown impact (no correlation)	Low	2774	1	7	2	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_User_Agent	Unknown impact (no correlation)	Low	2750	1	7	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Server_ID	Unknown impact (no correlation)	Low	1831	1	6	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_GetArg	Unknown impact (no correlation)	Low	425	1	6	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
FTP_Server_Identity	Unknown impact (no correlation)	Low	50	1	3	1	2006-09-06 14:00:00 EDT	2006-09-06 15:00:00 EDT
HTTP_Post_Field	Unknown impact (no correlation)	Low	48	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
FTP_User	Unknown impact (no correlation)	Low	38	1	3	1	2006-09-06 14:00:00 EDT	2006-09-06 15:00:00 EDT
HTTP_Cookie	Unknown impact (no correlation)	Low	35	1	4	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
FTP_Pass	Unknown impact (no correlation)	Low	32	1	3	1	2006-09-06 14:00:00 EDT	2006-09-06 15:00:00 EDT
SSH_Version	Unknown impact (no correlation)	Low	11	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Post	Unknown impact (no correlation)	Low	9	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_Authentication	Unknown impact (no correlation)	Low	7	1	2	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
TCP_Probe_HTTP	Unknown impact (no correlation)	Low	6	1	4	2	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT
HTTP_RobotsTxt	Unknown impact (no correlation)	Low	1	1	1	1	2006-09-06 14:00:00 EDT	2006-09-06 14:00:00 EDT

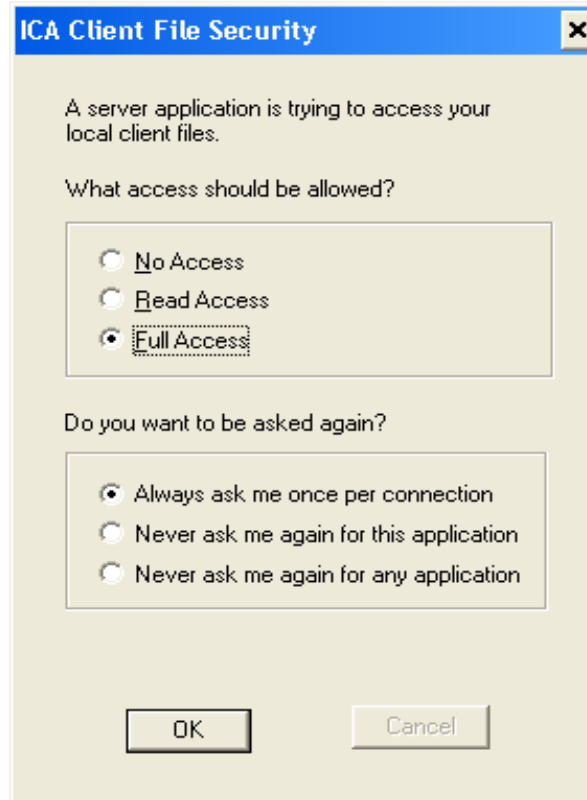
Remote Anonymous Ownership

- 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

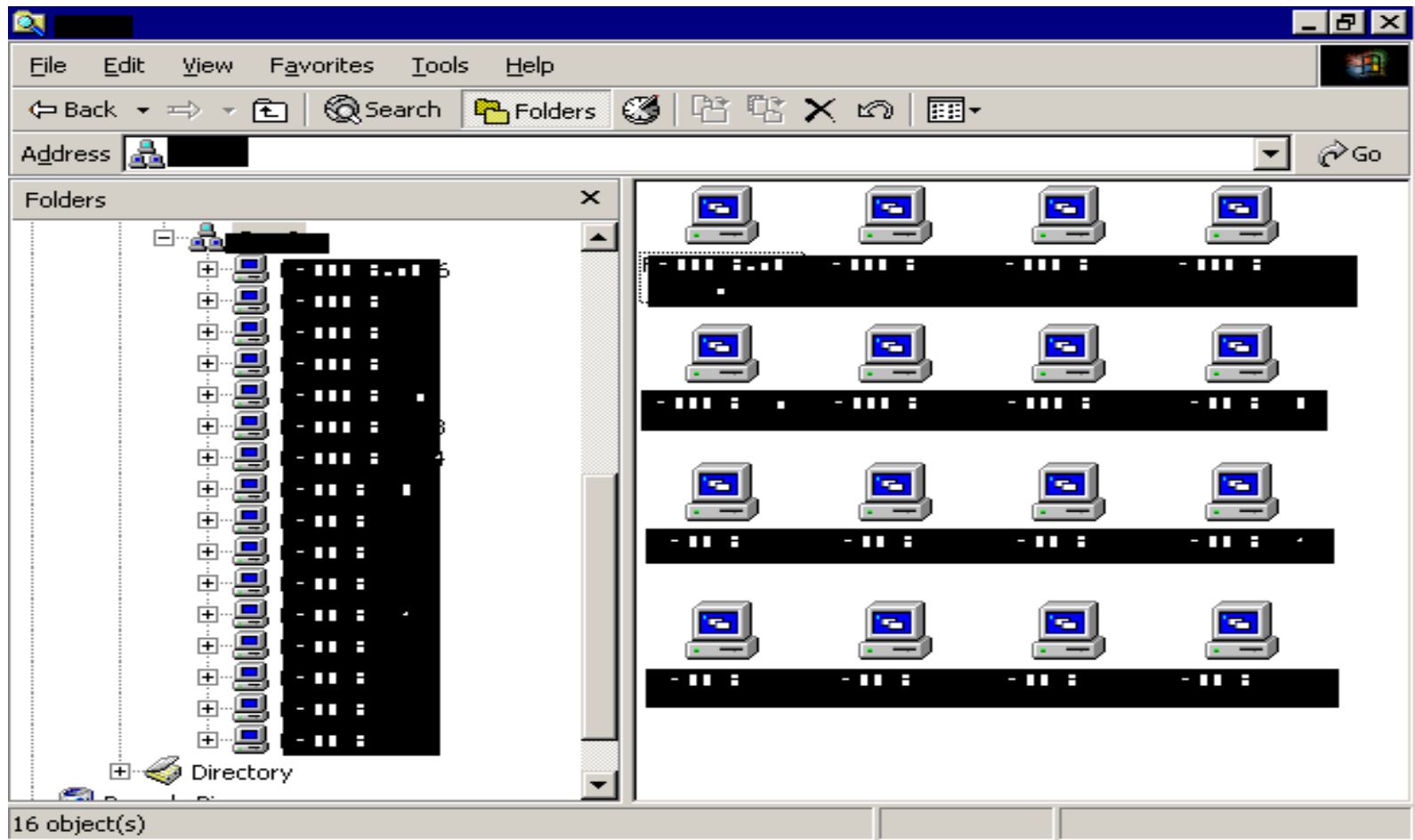
Remote access please!



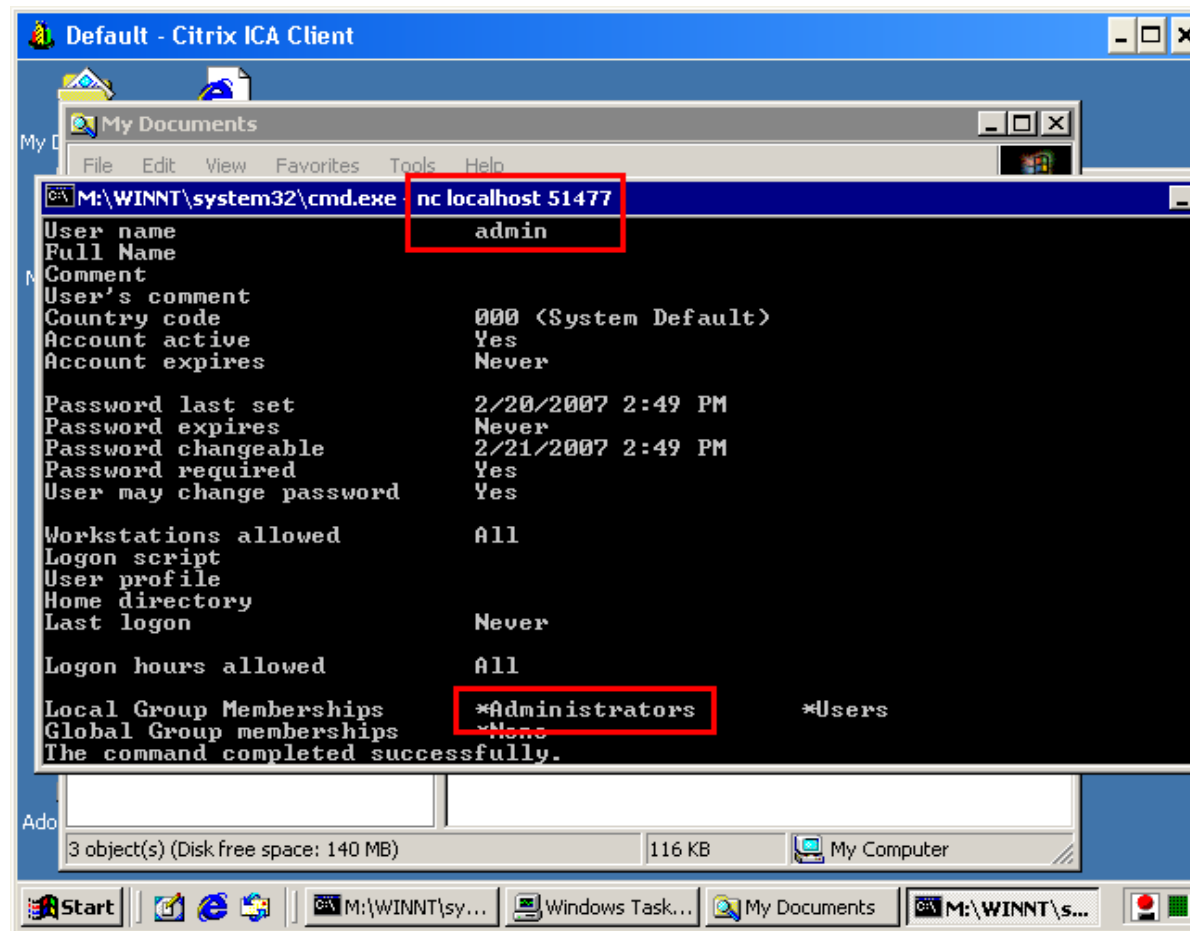
File sharing is nice too...



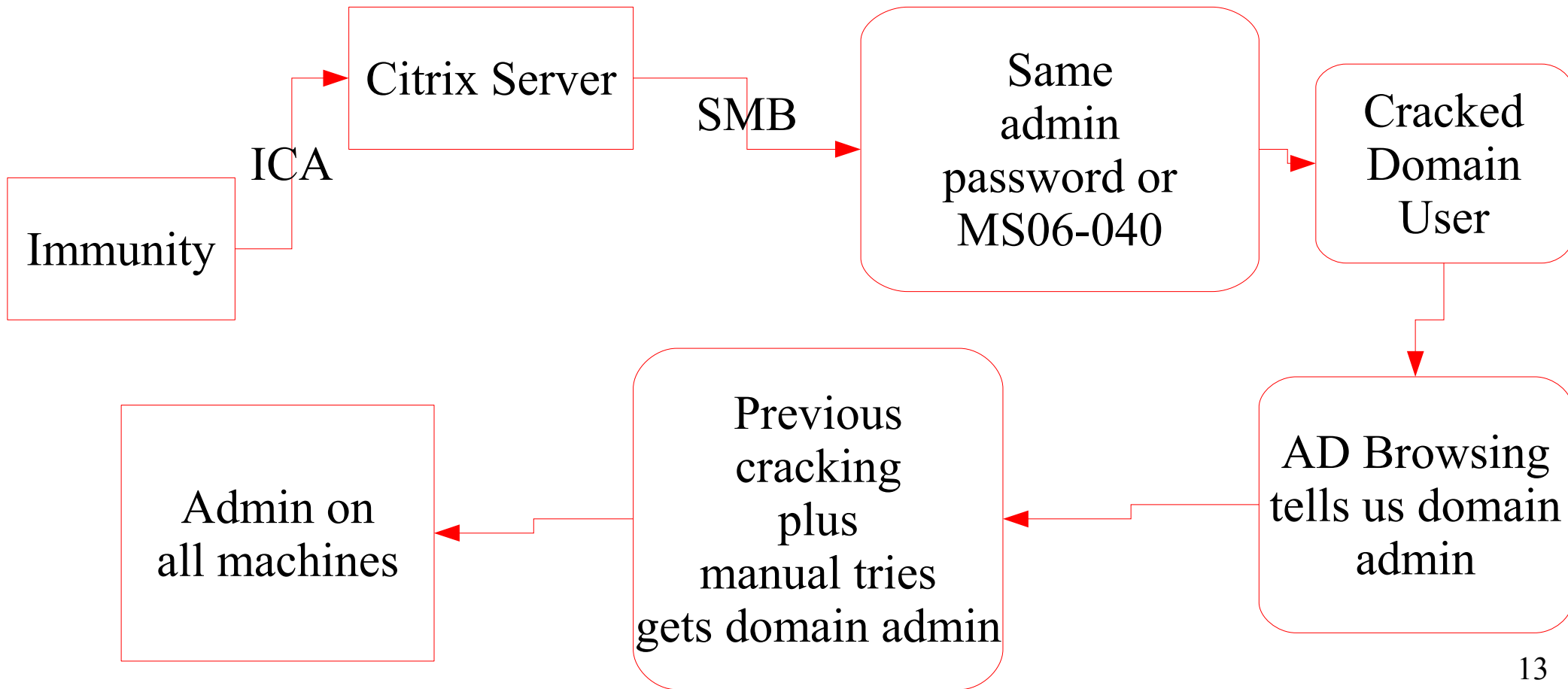
Lots of machines to see now



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

Oday to Remote MOSDEF Shell!

```
kostya@kostya:~/CANVAS
Loadlibrary iphlpapi.dll = 77340000
[C] GetProcAddress_withmalloc: Found iphlpapi.dll!GetIpAddrTable at 773445b4
Checking to see if I succeeded
Win32/MOSDEF$ runmodule whoami -0 none:none
  [C] Running module: whoami

[C] Args: -0 none:none

Loading whoami ... [ ok ]
[C] secur32.dll!GetUserNameExA not in cache - retrieving remotely.

Using loadlibrary_withmalloc! (secur32.dll)
Loadlibrary secur32.dll = 7c340000
[C] GetProcAddress_withmalloc: Found secur32.dll!GetUserNameExA at 7c345474

Loading computername ... [ ok ]
[C] kernel32.dll!GetComputerNameA not in cache - retrieving remotely.

[C] GetProcAddress_withmalloc: Found kernel32.dll!GetComputerNameA at 7c5856c3

[C] Computer Name: {}
[C] Computer Name: ██████████
[C] Result: ██████████ \IUSR_██████████
Win32/MOSDEF$
```

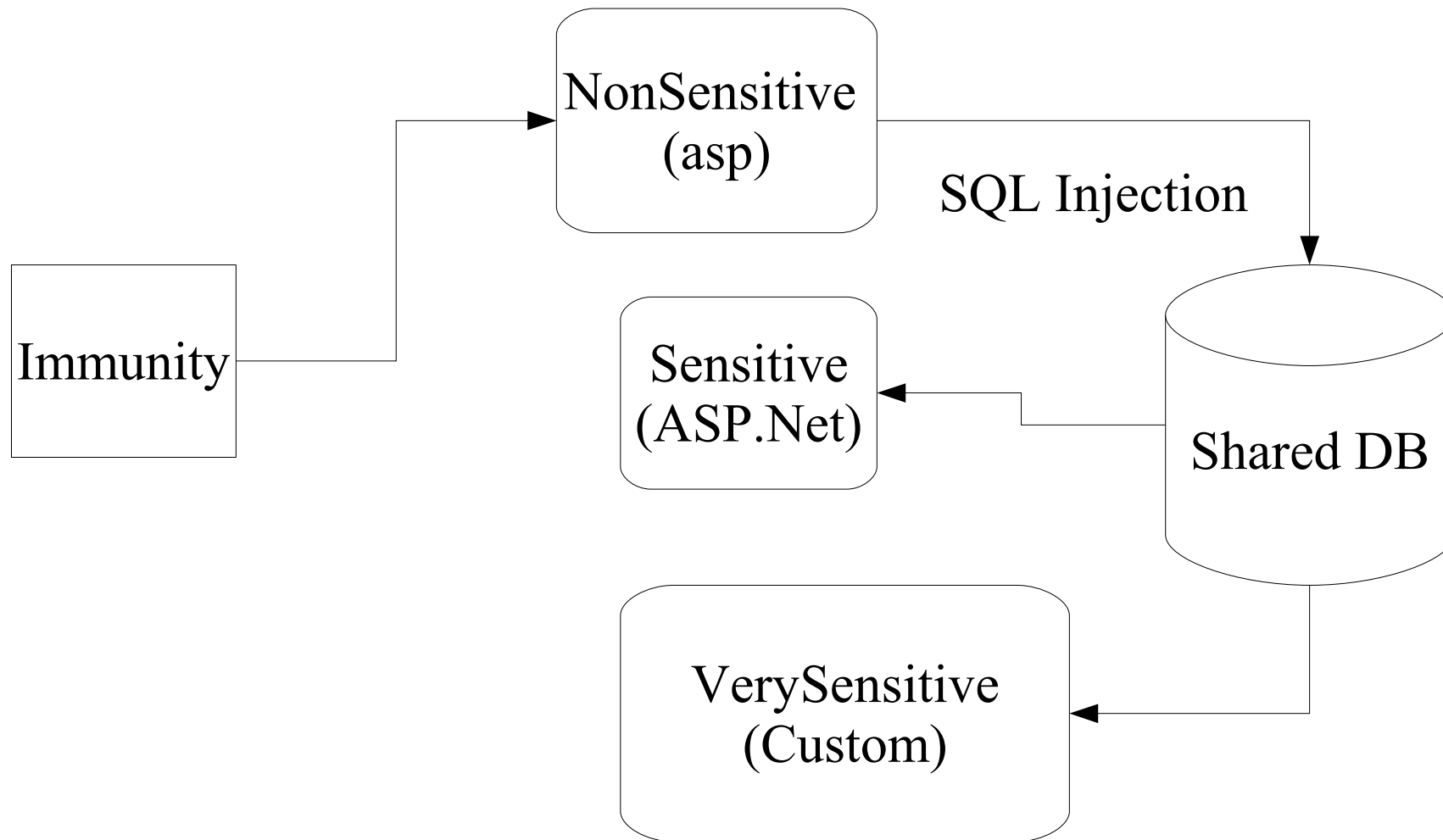

Sometimes a firewall will slow you down

- 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

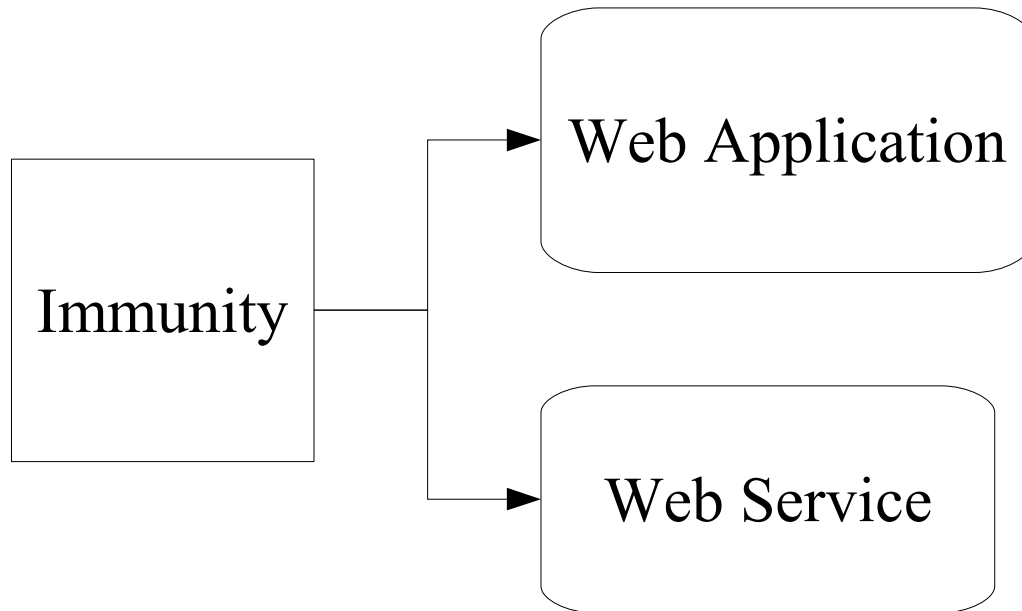
Results

- 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

- Oday 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



Security Research Team