

Security Trends & Tools 2007 **by Dayle Alsbury**

Top Security
Issues, Priorities and Tools

& SANS 2007 Alert Trend Analysis

Get Compliant.
Get TraceSecurity.

New Trends: 1Q - 2Q 2007

Mac OS/X

- Malicious parties following the herd, the trend
- 0-Day flaws are now being seen

Linux/Unix

- Linux flaws growing common place
- General Linux/Unix/Solaris/BSD flaws affecting services, applications and protocols

Windows OS

- Vuln announcements have spiked @ 7-8 weeks intervals
- High volume announcements typically contain Critical/High Level vulns. Low and Moderate trickle out.

New Trends: 1Q - 2Q 2007

Windows Services and Configuration

- Windows service configuration vulns widespread
- Widely circulated exploit code affecting Server Service, Exchange, etc...

Third Party Applications

- Proliferation of malware and botnets
- Recent moving average trending upwards in volume

Security, Enterprise and Directory Management Servers

- Compromise results in high level of access

New Trends: 1Q - 2Q 2007

DNS, Phishing, Spear Phishing, and more

- “Until recently, the security gap between mid- and large-market companies hasn't been an issue...But security experts agree that the number of cyber attacks on mid-market companies began rising last fall and continues to do so. The trend is clear.” – CIO Magazine 03/07

Vista User Account Control

- Disclosure of confidential information

Database Applications

- Two free tools to test your databases

New Trends: 1Q - 2Q 2007

Web Applications

- Common errors and vulns on the rise
- SQL and cross-platform attacks show event correlation

Excessive User Rights

- STILL a problem?!, why-oh-why!!

Poor ACLs

- More widespread than you might think

Signature Outsourcing

- Trend in outsourced R&D and why THAT'S a problem

Rise of the Virtual Machines

- Growing attention from they bad guys

MAC OS/X

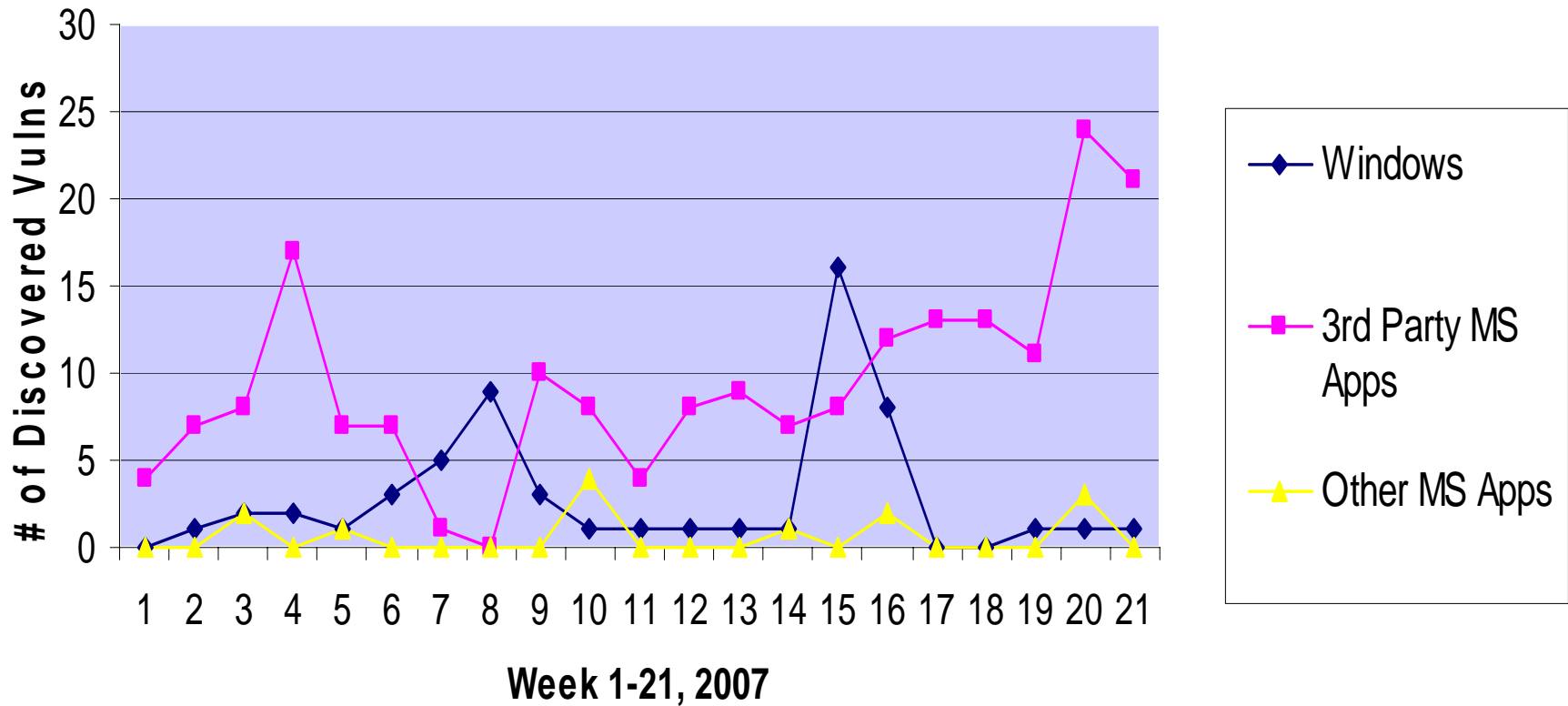
- Mac OS/X had its first reported Zero Day Attack
- ## UNIX-based
- Based on and contains large amounts of code from Unix-like OS
 - Safari users browsing a malicious web site had their computer automatically download and execute a malicious file. With no error other than to visit the web site.
 - Apple patched the Safari flaw, but had to issue a 2nd patch to stop another attack involving email attachments.

UNIX Vulnerabilities

- Unix 40 new vulns since January 1
- Linux 86 new vulns since Jan 1
- Solaris 17 new vulns
- HP-UX & Novell, both have 7 new vulns
- AIX 6 new vulns
- BSD 6 new vulns since January 1
- Sendmail MTA, Novell GroupWise Messenger, NetMail and SuSE Linux Enterprise server contain arbitrary code execution vulnerabilities
- Simply using *nix doesn't insulate you from vulnerability

SANS Windows Vulns Trends 2007

2007 Windows Trends



Windows Services and Configuration

A variety of Windows services are used to implement operating systems functions

- **Services.exe**

Some services provide remote interfaces to client components (RPC)

- Many vulnerabilities allow exploitation remotely and anonymously
- Exploitation of these services grant the same level of privilege.
- RPC flaws are typically very serious (CVE-2007-1748) and often affect key/critical functions such as DNS
- Block the ports 135-139/tcp, 445/tcp and other ports used by Windows systems at the network perimeter

Windows Services and Configuration

Critical vulnerabilities detected in Windows services over the past year:

- Routing and Remote Access Service
- Code execution and buffer overflow flaws are routinely identified
- Vulnerabilities in Windows libraries can be exploited in multiple vectors. In many cases a remote attacker will just need to persuade a user to access a specially crafted website, image, icon, or cursor file and the attacker would be able to execute arbitrary code on that user's system, with their privileges.
- Each of these vulnerabilities is remotely exploitable and grants full system privileges
- Vista denial-of-service. and protocol vulnerability and security escalation flaws already in circulation (CVE-2007-1528, CVE-2007-1530. Vista mail client-side file execution, etc.)

Windows Configuration Weaknesses

User configured password weakness

- One of the oldest and most important problems facing IT
- Assists in the proliferation of botnets, malware and spyware

Service account passwords

- Necessary for non-system services to have passwords
- Requirements for these passwords allow short, easily printable passwords
- Services often provide high level privileges

Null log-on

- Allows anonymous enumeration of accounts, shares and systems

Windows Configuration Weaknesses

Protection

- Implementation of strong passwords for user accounts
 - At least six characters
 - Combination of uppercase and lowercase letters, numerals and symbols
- Prevent Windows from storing the LM hash in the SAM database or Active Directory
 - support.microsoft.com/default.aspx?scid=KB;EN-US;q299656&
- Implement a policy to regularly check for weak passwords
- Use strong passwords for services such as IIS, BackupExec and SQL
- Restrict anonymous access to domain systems

WIN Config Testing Tools

WMIC (Win Mgt Instrumentation Cmd)

- CLI tool uses WIN query language to provide local and remote WIN info
- WMIC has scripting ability
 - HEY, it's no cost continuous auditing!!!!
- VERY good FREE tool to automate auditing of patch management program
- VERY good FREE tool to show active accounts and the last time passwords were changed! *Restrict anonymous access to domain systems

www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/wmic.mspx

WIN Testing with WMIC qfe

```
FixComments=Update
HotFixID=KB928255
InstallDate=
InstalledBy=SYSTEM
InstalledOn=2/15/2007
Name=
ServicePackInEffect=SP3
Status=

Caption=
CSName=DBCUZ3B1
Description=Security Update for Windows XP (KB928843)
FixComments=Update
HotFixID=KB928843
InstallDate=
InstalledBy=SYSTEM
InstalledOn=2/15/2007
Name=
ServicePackInEffect=SP3
Status=

Caption=
CSName=DBCUZ3B1
Description=Update for Windows XP (KB931836)
FixComments=Update
HotFixID=KB931836
InstallDate=
InstalledBy=SYSTEM
InstalledOn=2/15/2007
Name=
ServicePackInEffect=SP3
Status=

Caption=
CSName=DBCUZ3B1
Description=High Definition Audio Driver Package - KB835221
FixComments=Update
HotFixID=KB835221WXP
InstallDate=
InstalledBy=Administrator
InstalledOn=6/9/2006
Name=
ServicePackInEffect=SP10
Status=

C:\>
```

Microsoft Office

Attackers exploit targets by:

- Sending the malicious Office document in an email message
- Hosting the document on a web server or shared folder, and entice a user to browse the webpage or shared folder.
- Running a news server or hijacks a RSS feed that sends malicious documents to email clients

Easy fix...

- Disable Internet Explorer feature of automatically opening Office documents.
- Configure Outlook and Outlook Express with enhanced security

3rd Party Apps: Instant Messaging and P2P

Files and data viewable to the Internet at large

- Shared documents and files in the P2P network may be accessible to others on the network

Proliferation of malware and botnets

- Unknowingly downloading malware and spyware, accepting files from unknown users

Disclosure of confidential information

Legal liability

3rd Party Apps: Media Players

Apple QuickTime, iTunes, Windows Media Player, RealNetworks RealPlayer, Nullsoft Winamp and Adobe Macromedia Flash contain buffer overflow and memory corruption vulnerabilities.

- Apple QuickTime/iTunes
 - **CVE-2005-2340, CVE-2005-2753, CVE-2005-2754, CVE-2005-2756, CVE-2005-3707, CVE-2005-3708, CVE-2005-3709, CVE-2005-3711, CVE-2005-3713, CVE-2005-4092**
- Windows Media Player
 - **CVE-2006-0005, CVE-2006-0006**
- Nullsoft Winamp
 - **CVE-2005-3188, CVE-2006-0476, CVE-2006-0720**
- RealNetworks RealPlayer
 - **CVE-2005-2629, CVE-2005-2630, CVE-2005-2922, CVE-2005-3677, CVE-2006-0323**
- Adobe Macromedia Flash Player
 - **CVE-2005-2628, CVE-2006-0024**

3rd Party Apps: Backup Software

These vulnerabilities can be exploited to completely compromise systems running backup servers and/or backup clients. An attacker can leverage these flaws for an enterprise-wide compromise and obtain access to the sensitive backed-up data.

- Veritas: **CVE-2005-3116, CVE-2006-0989, 0990 & 0991**
- EMC Legato: **CVE-2005-3658 & 3659**
- CA ARCserve: **CVE-2006-5142 & 5143**

Security, Enterprise and Directory Management Servers

Spam and virus filters can often be exploited by specially crafted email messages

- Compromise can be used to retrieve additional accounts

Configuration and patching systems

- Compromising these systems provides an easy path to further distribute malware

Snort detection vulnerabilities; detection code has overflow vulnerabilities (2005) www.securityfocus.com/bid/15131

Feb 2007 Snort DCE/RPC pre-processor
osvdb.org/displayvuln.php?osvdb_id=32094

Security, Enterprise and Directory Management Servers

DM servers provide a high level of access and privilege

- Used to maintain a large amount of user and system information

Often configured with weak passwords

- Acquiring hashes to these passwords may result in compromise of a large number of systems

Often configured to use unencrypted transmission

Often expose SMB data/shares

- One of the most critical and overlooked controls
- Wide open LAN SAM database/share access

Excessive User Rights

Important to balance convenience and security

Unauthorized and/or infected devices on the network

- Laptops, USB drives
 - May contain Trojans or viruses which spread to the rest of the network
- Rogue access points
 - Provide wireless access to unknown entities on the outside

Excessive user rights and unauthorized software

- Ability to install unauthorized software such as Peer to Peer file sharing programs, IM software and games
- Malware allowed onto the system through unauthorized software will likely install additional unauthorized software

Let's go Phishing

Phishing

- Users are directed to enter their information in a fake website setup to look like a banking or online sales site
- Information is captured and identity is stolen

VoIP Phishing

- New form of Phishing in which users are directed to call a number and enter personal information such as bank PINs or passwords

Spear Phishing/Social Engineering

- Highly targeted attacks which involve large amounts of preparation and information about the organization

Auto-Phishing

- Bot infected system sends an auto-reply email from a legit user to a legit user with payload or link to phishing site.

DNS Servers & Phishing

Increasingly, the following types of attacks are carried out by botnets against DNS servers.

- **Recursion Denial of Service Attacks**
 - A Botmaster publishes a large DNS record in a compromised DNS server and then directs the botnet to send small UDP/53 queries to public recursive name servers with a forged return address pointed at the targeted victim. Result = the recursive DNS servers, rather than the bots, directly attack the victim.
- **Spoofing Authoritative zone Answers**
 - The botmaster establishes a fake web site (phishing site) on a compromised web server. The botmaster then directs the botnet to listen for requests and spoof DNS replies for a particular zone with an answer pointing to the compromised web server. This is very commonly deployed in tandem with a Phishing Attack.

Vista and User Account Control (UAC)

User Account Control is designed to:

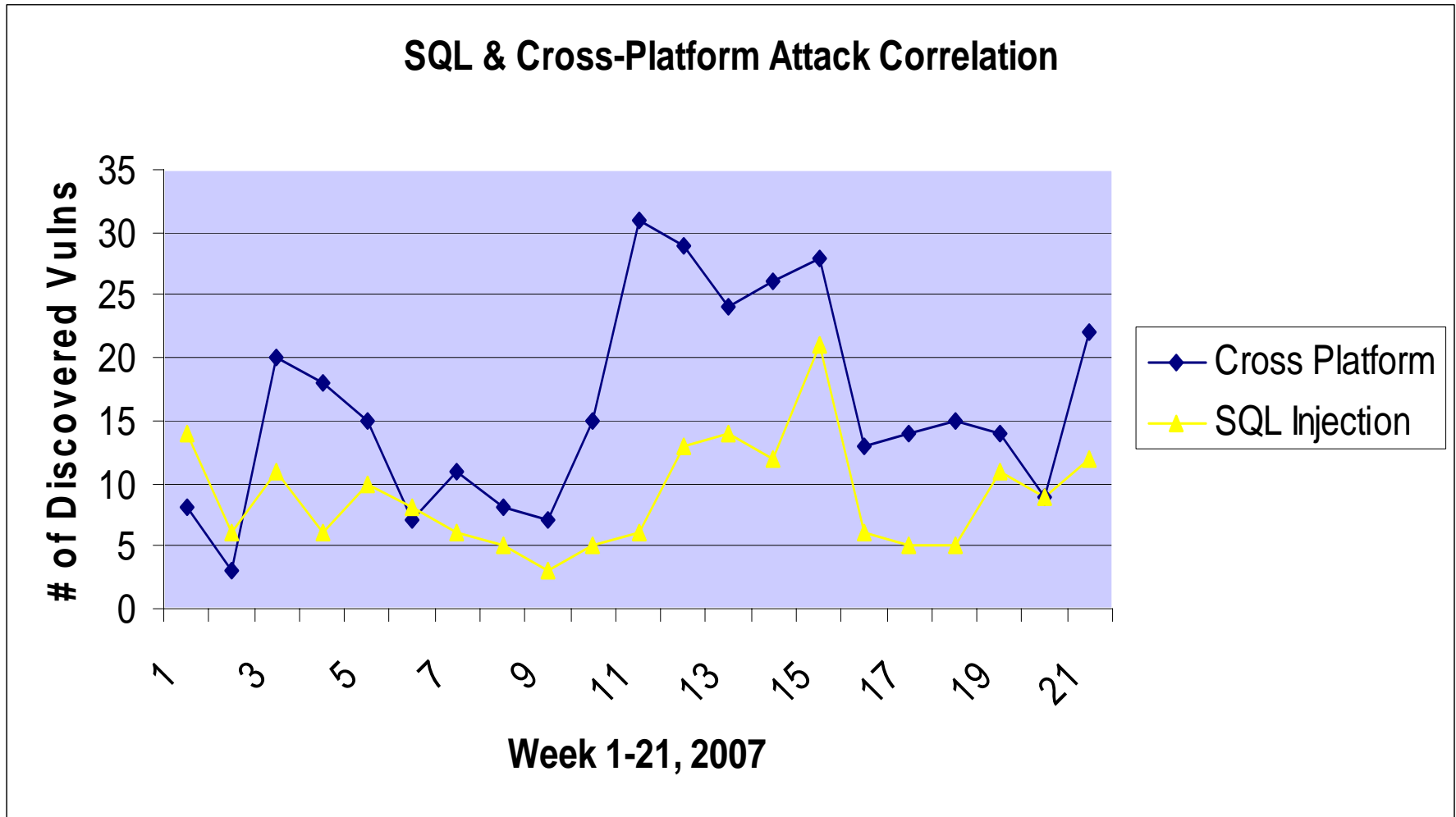
- Attempts to limit vulnerability exposure by restricting user account privileges via Integrity Levels (improvement over XP)
- Cannot modify processes with higher integrity levels
- Integrated with other Vista security features such as Security Policy MMC and Group Policy.
- Thankfully, this has forced application developers to begin writing applications to run in Standard User Mode (more secure than XP Admin mode).
- No more Found New Hardware Wizard auto-prompts (yay)
- But, UAC is NOT security, it is user control....

Vista and User Account Control (UAC)

UAC Problems

- Verbose response prone to creating routine behavior
 - Always answer 'yes', just to make it go away
- Tools to override/silence UAC pop-up notification already in circulation
 - Tweak-UAC and other tools freely available for download
- Assumes all installs should run in Administrator mode
- CAN modify processes with same/lower integrity levels
- Malware can't modify the registry, but it can write to the automatic startup directory
- Chml is a new utility tool that allows you to manage Windows Integrity Levels
 - <http://www.minasi.com/vista/chml.htm>

SANS SQL & Cross-Platform Correlation



Web Applications

- SQL injection 139 during 2nd ½ of 06
 - SQL injection 188 during first 21 wks of 07
 - Cross-site scripting 376 ('06), 141 so far in 2007
- phpBB, MediaWiki, Horde, PHPMyAdmin, Mambo vulns can be easily exploited to execute arbitrary PHP code and/or arbitrary back-end database commands.
- Bots incorporate these exploits quickly and these attempts are among the most frequent attacks
 - Over 300 Cross-Platform Attacks (XPA) so far in 2007
 - Compromise in credentials in one platform leads to compromise of another. Increasing use of centralized authentication models have increased WIN credentials compromise.
 - Almost 600 Web App vulns so far in 2007

Web Applications

Common Errors

- Default content & files left unsecured
- Directory listing capabilities unsecured
- Poor permissions
- Failure to use block HTTP requests based upon configured rules
- Information disclosure: OS headers, internal IP addresses, log files, etc.
- Lack of input, error code sanitization and field checking
- Not hard to test: Nikto, Wikto, etc. (Linux tools)
 - www.cirt.net/code/nikto.shtml

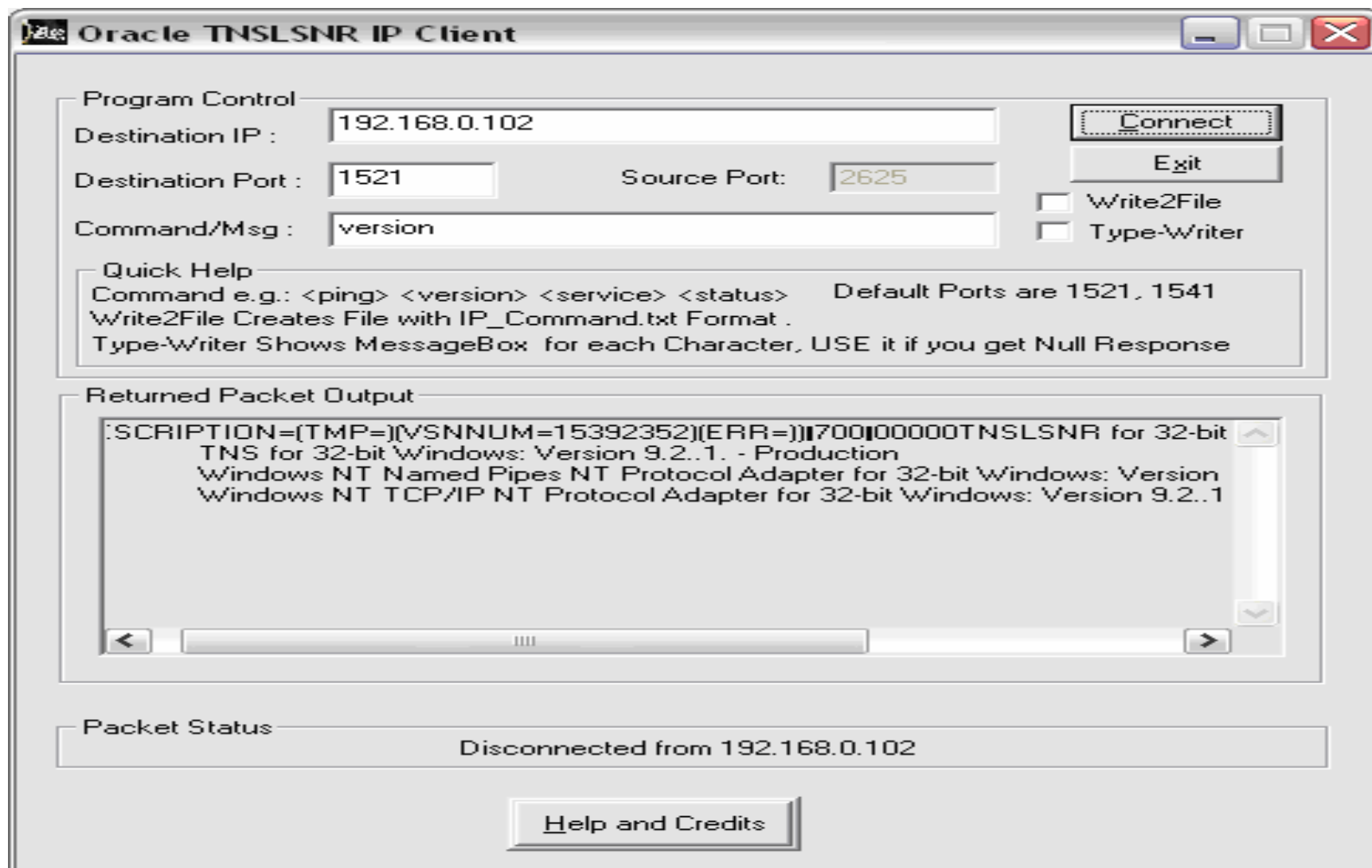
Predeployment Test Your WebApp with Nikto

```
- Nikto 1.35/1.34 - www.cirt.net
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 80
+ Start Time: Thu Feb 22 09:51:34 2007
-----
----
- Scan is dependent on "Server" string which can be faked, use -g to
override
+ Server: Microsoft-IIS/6.0
- Retrieved X-Powered-By header: ASP.NET
+ OSVDB-630: IIS may reveal its internal IP in the Location header via
a
request to the /images directory. The value is
"http://172.16.168.168/images/". CAN-2000-0649.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD HTTP method 'TRACE'
is
+ typically only used for debugging. It should be
disabled. OSVDB-877.
+ Microsoft-IIS/6.0 appears to be outdated (4.0 for NT 4, 5.0 for
Win2k)
+ /clusterframe.jsp - Macromedia Jrun 4 build 61650 remote
administration interface is vulnerable to several CSS attacks. (GET)
+ /modules.php?name=Members_List&letter=All&sortby=pass - PHP Nuke
module allows user names and passwords to be viewed. See
http://[REDACTED] PHP-Nuke6.0-Members List-Your Account.txt
for other SQL exploits in this module. (GET)
+ /css - Redirects to [REDACTED] This might be
interesting...
+ /js - Redirects to [REDACTED] , This might be
interesting...
+ /url.jsp - This might be interesting... has been seen in web logs
from
an unknown scanner. (GET)
+ 14915 items checked - 3 item(s) found on remote host(s)
+ End Time: Thu Feb 22 10:29:32 2007 (2278 seconds)
```

Database Applications

- Vulns on Oracle and Sybase EAServer
- Oracle: 2 cumulative security patches in January and April fixes many buffer overflows, SQL injections and privilege escalation vulns
 - TNSLSNR vuln and account enumeration most common vulns found
 - www.vulnerabilityassessment.co.uk/oracletnslnr.htm
- Sybase EAServer
 - Exploit code targeting a buffer overflow vulnerability has been publicly released.

Test Oracle with TNSLSNR Tool



Test Oracle with TNSLSNR Tool

-] Checking host 192.168.7.238
-] Checking sid (na4bb) for common passwords
-] Account DBSNMP/DBSNMP found
-] Enumerating system accounts for SID (na4bb)
-] Successfully enumerated 7 accounts
-] Account OUTLN/OUTLN found
-] Account SYS/CHANGE_ON_INSTALL found
-] Account SYSTEM/MANAGER found
-] Checking user supplied passwords against sid (na4bb)
-] Checking user supplied dictionary
-] Account JMS/JMS found
-] Account NETACT/NETACT found
-] Querying database for version information

Test Microsoft SQL Servers

SQLRecon: www.specialopssecurity.com/labs/sqlrecon

SQLat: www.cqure.net/wp

Both test MS-SQL servers for obvious passwords.

- IE: sa-sa

SQLat contains a suite of enumeration, dumps, password crack and file upload tools against a MS-SQL server.

Good tool to audit your how well your DBs secure their MS-SQL databases

Test MS SQL db with SQLRecon

The screenshot displays the SQLRecon v1.0 application window. The interface is divided into several sections:

- Header:** "SQLRecon v1.0" and "SPECIAL OPS SECURITY".
- Menu:** "File" and "Help".
- Scan Options:**
 - Scan Type:** Radio buttons for "Active (IP Range)" (selected), "Active (IP List)", and "Stealth".
 - IP Range:** "Start:" field contains "192.168.0.101", "End:" field contains "192.168.0.102". Buttons for "Clear", "Dns Lookup", and "1..254".
 - IP List:** An empty text box with a "Browse" button.
 - A "Scan" button is located at the bottom of the options panel.
- Results:** A tree view showing scan results for "192.168.0.102 [LAB-WIN2000SERV] [8.0.311 (guess)]".
 - ServerIP : 192.168.0.102
 - TCP Port : 1433
 - ServerName : LAB-WIN2000SERV
 - InstanceName : MSSQLSERVER
 - BaseVersion : 8.00.194
 - SSNetlibVersion : 8.0.311
 - TrueVersion :
 - ServiceAccount :
 - IsClustered : No
 - Details
 - (UDP)ServerName;LAB-WIN2000SERV;InstanceName;MSSQLSE
 - DetectionMethod : UDP
- Footer:** "Scan Complete (1 instances found.)"

Poor Access Control List configs

Poor Access Control List configuration

- Inconsistent ACL configuration
- Lacking ACL baseline configurations
- Lacking standardized ACLs

Cisco Router Audit Tool

- Free command-line ACL scoring tool
- Helps identify logic and configuration errors
- Helps ensure standardization through baseline configuration & quantifiable scoring
- www.cisecurity.org/bench_cisco.html

Cisco RAT Output

Router Audit Tool report for
192.168.0.200
Audit Date: Thu Mar 8 20:17:22 2007 GMT
Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - login default	192.168.0.200		
10	pass	IOS - enable secret	192.168.0.200		
10	FAIL	IOS - require line passwords	192.168.0.200	con 0	72
10	FAIL	IOS - no snmp-server	192.168.0.200	snmp-server engineID local 0000000902000002B91D8643	2
10	FAIL	IOS - no snmp-server	192.168.0.200	snmp-server community public RO	2
10	FAIL	IOS - no snmp-server	192.168.0.200	snmp-server community private RW	2
10	FAIL	IOS - no ip http server	192.168.0.200	n/a	60
10	FAIL	IOS - forbid SNMP read-write	192.168.0.200	private	70
10	FAIL	IOS - forbid SNMP community public	192.168.0.200	n/a	63
10	FAIL	IOS - forbid SNMP community private	192.168.0.200	n/a	64
10	FAIL	IOS - apply VTY ACL	192.168.0.200	vtty 0 4	75
10	FAIL	IOS - Use local authentication	192.168.0.200	n/a	2
10	FAIL	IOS - Define VTY ACL	192.168.0.200	n/a	2
10	FAIL	IOS - Create local users	192.168.0.200	n/a	2
7	pass	IOS 12 - no udp-small-servers	192.168.0.200		
7	pass	IOS 12 - no tcp-small-servers	192.168.0.200		
7	pass	IOS 12 - no directed broadcast	192.168.0.200		

Cisco RAT Output

file:///C:/tools/CIS/RAT/bin/192.168.0.200.html

file:///C:/tools/CIS/RAT/bin/192.168.0.200.html | file:///C:/tools/CI...192.168.0.200.html

5	FAIL	IOS - line password quality	192.168.0.200	vty 0 4	76
5	FAIL	IOS - line password quality	192.168.0.200	con 0	72
5	FAIL	IOS - VTY transport telnet	192.168.0.200	vty 0 4	75
3	pass	IOS - logging trap info or higher	192.168.0.200		
3	pass	IOS - disable aux	192.168.0.200		
3	FAIL	IOS - logging console critical	192.168.0.200	n/a	2
3	FAIL	IOS - clock timezone - GMT	192.168.0.200	n/a	2

Summary for 192.168.0.200

#Checks	#Passed	#Failed	%Passed
41	13	28	31

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
283	83	29

Overall Score (0-10)
2.9

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

Fix Script for 192.168.0.200

Done

Proxy: None (unknown) none

NASL & Signature Outsourcing

IDS/IPS Signature Patterns

- Signatures based upon matching exploit code patterns
- Signatures also search for unique identifiable triggers
- Evil H@x0r adjusts his/her code to deliver the payload without matching the search pattern.
- Evil H@x0r's payload is not confined by the host. He/she simply alters the host code structures or payload size to bypass the signature pattern.
- Evil H@x0r now uses 'packers' for rapid code mutation. No need to write new code for each variant. The 'packer' continually mutates the exploit and repacks it for propagation. IDS signatures can't keep up!

NASL & Signature Outsourcing

IDS/IPS Signature Patterns

- Signatures also key off of the memory code jump point
 - Code instructions to jump from one memory point to another
- Evil H@x0r substitutes the 'jump' point of the vulnerability for that of an infrequently used memory point that will execute the same transaction.
- An increasing number of IDS/IPS companies are outsourcing signatures to a few firms. As this practice grows, Evil H@x0r will begin to be able to pattern the types of exploits with the highest probability of bypassing IDS.
- BEWARE, uniform, assembly-line IDS sigs will lead to a false sense of security.

Rise of the Virtual Machines

Virtual Machines = cost effective but vulnerable

- Targeted because compromise yields multiple successes
- Antispyware/anti-malware difficulty scanning virtual environments.
 - Virtual memory space and tables cannot be easily read from physical machine environment
- VMs typically run with high privileges due to need for comprehensive host access to hardware layer
- A virtual machine buffer overflow may allow the bad guys to compromise both the virtual and host machines
- A VM 'escape' flaw attack allows a hacker to escape the virtual environment and execute code in the host env.

Notes

Continuous patching by criticality
Proactive configuration management
Test prior to roll-out
Continuous auditing
Secure the 'human element'
Stay informed

- www.sans.org,
- www.cert.org/advisories,
- www.securityfocus.com
- www.nsa.gov/snac
- dayle@tracesecurity.com