

Rimell Associates Ltd.

(Some) IT Security Threats
or
How afraid would you like to be?

Steve Rimell
steve@rimell.com

Rimell Associates

The top issues of 2009-10

- Inadequate patching
- SQL injection
- Abuse of system/access privileges
- Default credentials
- Loss of data/equipment
- Phishing and its variations
- Denial of Service
- Insecure networks

Patching

- Patching – the installation of software updates to fix a problem or address a security risk
 - All software needs to be patched
 - Gartner Group once estimated one bug remains for every 1500 lines of source code, even after 'full' testing and debugging.
 - Windows Server 2008 has over 95 million lines of code – go figure...

3

Patching

- Why is it a problem?
 - There can be a lot of patches – MS has regular cycle ('Patch Tuesday'). Other vendors have their own arrangements
 - Patches may be released in large numbers and can be 'out of cycle' to address urgent issues
 - If you have a lot of systems from different vendors, you have a huge patch tracking problem
- ⑩ But the main problem – patches can break things!

4

Patching - The 'zero-day' exploit

- Patches are created to address known vulnerabilities, so in the ideal world:
 - ◆ Weakness is discovered
 - ◆ Vendor notified
 - ◆ Vendor confirms weakness exists
 - ◆ Vendor creates security patch
 - ◆ Vendor notifies everyone
 - ◆ Patch is distributed
 - ◆ Patch is installed by all users
 - ◆ Hacker attack is prevented – all is well

5

Patching - The 'zero-day' exploit

- What really happens...
 - ◆ Weakness is discovered
 - ◆ Hacker creates exploit and puts it on YouTube
 - ◆ Millions of script kiddies download exploit and start using it
 - ◆ Vendor notified
 - ◆ Vendor confirms weakness exists
 - ◆ Vendor creates security patch
 - ◆ Vendor notifies some of us, but not everyone finds out in time
 - ◆ Patch is distributed incompletely
 - ◆ Patch is installed by some users
 - ◆ Hackers attack vulnerable systems

6

Patching questions

- We need to address these issues:
 - How do we find out that a vulnerability exists?
 - How do we find out that a patch exists for the vulnerability?
 - Can we obtain the patch from a secure, trusted source?
 - Is the patch actually required for our systems?
 - How do we test it and for how long?

7

Patching questions for the auditor

- Patching issues (cont)
 - How do we distribute the patch?
 - Is it safe to patch all our systems at once?
 - ◆ If we do, and the patch goes wrong (not unknown), we have crippled our systems
 - ◆ If we don't, we are leaving some of our systems open to attack
 - How do we 'undo' the patch if it causes problems after installation?
 - How do we handle downtime? Many Windows patches require a restart

8

Patching questions

- Patching issues (cont)
 - How do we patch?
 - Windows has automatic updates, but we can't use it in a production environment
 - MS has their own solutions (MOM, SMS, WSUS)
 - What about other vendors?
 - What about the applications (Adobe Reader, Flash etc.)?

9

Patching questions

- Patching issues (cont)
 - What about our infrastructure devices (hubs, routers, switches, firewalls etc? – they all have their own built-in OS, and have all been subject to attack.
 - Is there any way of centralising patch management to ensure completeness and accuracy when you do patch? Does the IT department know the extent of your inventory and what needs to be done?

10

Patching questions

- For the local/central government people:
 - Don't forget your responsibilities under the Code of Connection – version 4.1 says that these are a MUST:
 - ♦ A patch management policy is in place and documented for all software (including firmware) used on the network
 - ♦ Patches are applied in a timely fashion and audited to ensure compliance. Please state your Organisation's patch delay time (e.g. from a patch being issued, identified as critical/ patch requires to be applied, tested, installed, verified etc) when applying usability, fault and security patches.

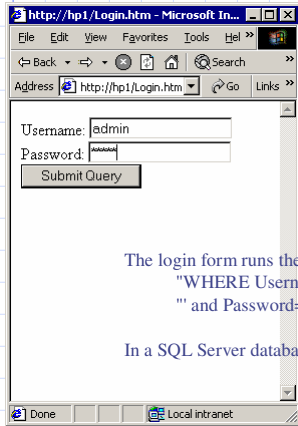
11

SQL injection

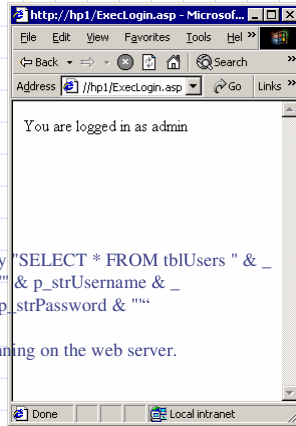
- We thought this problem was fixed but it's not..
 - SQL injection – the subversion of a database application by causing it to run a query or command that is logical but not sensible.
 - Exploits the inability of some system designers to build proper input sanitation into their application.

12

Example of a simple login form



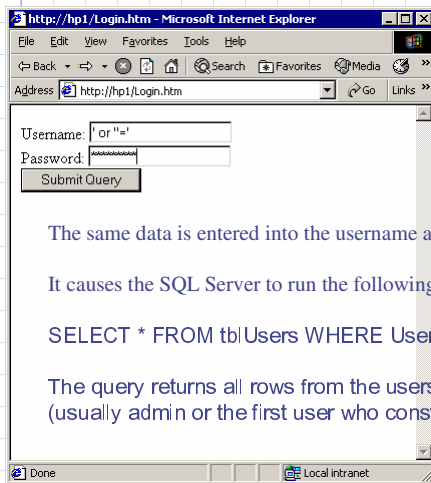
The login form runs the query "SELECT * FROM tblUsers " & _
 "WHERE Username='" & p_strUsername & _
 "' and Password='" & p_strPassword & ""
 In a SQL Server database running on the web server.



Contents of tblUsers

Username	Password
admin	admin
steve	train
guest	password

SQL Injection

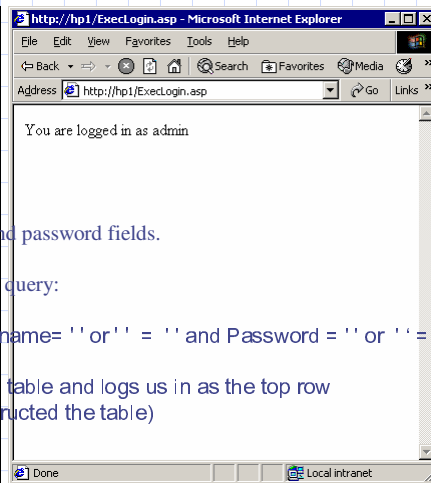


The same data is entered into the username and password fields.

It causes the SQL Server to run the following query:

```
SELECT * FROM tblUsers WHERE Username= ' or ''=' and Password = ' or ''='
```

The query returns all rows from the users table and logs us in as the top row (usually admin or the first user who constructed the table)



Other SQL injection horrors

`http://www.example.com/Article.asp?ID=0 or 1=1`

`http://www.example.com/Article.asp?ID=1055; DELETE FROM tblArticles`

`' exec master..xp_cmdshell 'net user test testpass /ADD' --`

15

SQL Injection remedies

- If a user is asked to input a number, verify the data type
- For string data, replace single quotes with two single quotes
- Use stored procedures to abstract data access so that users do not directly access tables or views
- Establish strong coding standards involving code review and peer-test often

16

Abuse of system/access privileges

- A common scenario in your organisation?
 - Use needs to carry out some non-standard task
 - The task requires some subtle adjustment to access rights and privileges that is very complicated to work out
 - Quicker and to give the user administrative access rights 'just until the problem is solved'
 - Of course, they're always removed again afterwards?

17

Abuse of system/access privileges

- Common examples:
 - Membership of the Windows Domain Admins group
 - Use of the 'root' account in UNIX
 - Use of the 'sa' account in SQL Server/Sybase
 - The Oracle SYSTEM account

18

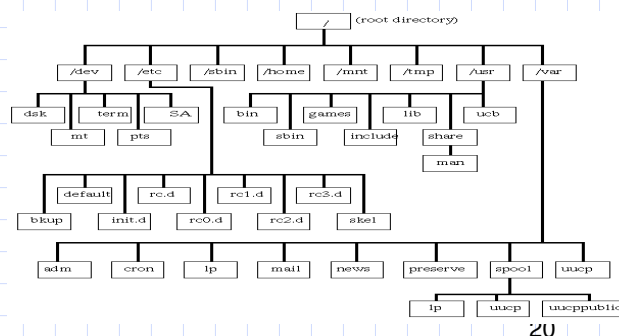
Abuse of system/access privileges

- Possible countermeasures?
 - Windows:
 - ◆ Use the 'restricted groups' feature
 - ◆ Use Delegation of Control
 - UNIX
 - ◆ Sudo, Role Based Access Control
 - SQL Server, Sybase, Oracle
 - ◆ Integrated Authentication, database roles, use of system privileges

19

Abuse of system/access privileges

- What's the risk if you don't control access rights?
 - ◆ There's no better example than the famous 'rm -rf *' command in UNIX, but all operating systems can suffer the same fate.



Default credentials

- All systems and devices have to go through an initial setup phase after installation
- They all have standard user/password combinations to get you started
- Examples:
 - The SYSTEM/MANAGER exposure in Oracle
 - The 'sa' account in SQL Server
 - The Cisco/engineer authentication weakness
 - Etc, etc, etc...

21

Default credentials

- The problem – everybody knows these default credentials
 - If you don't, just Google for dpl.htm (default password list for all kinds of devices)
- ⑩ The countermeasure – easy to recommend, but not so easy to implement – change all the default credentials and set up a periodic change policy.

22

Loss of data/equipment

- According to Secure Computing Magazine
 - 10,000 mobile phones are left in London taxis every month, and 1,000 other hand-held devices
 - Over three quarters of businesses have regular remote users among their workforce, yet only 27 per cent use hard disk encryption.
 - According to survey by Check Point, 77 per cent of businesses have a quarter of staff who regularly work remotely, and in addition, only nine per cent use encryption for removable storage devices.

23

Loss of data/equipment

- A £500,000 penalty has been introduced by the Information Commissioner's Office (ICO) for personal data security breaches.
- There are plans to increase the punishing powers of the ICO and an announcement revealed that it will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act.

24

Loss of data/equipment

- The obvious countermeasures:
 - Hard disc encryption
 - Encrypted removable storage devices
 - Boot sector protection for laptops
- ⑩ Reports claiming that hardware-encrypted USB flash drives were hacked earlier this year have revealed a major flaw in the products' design.

25

Loss of data/equipment

- So, don't take their word for it – make sure the security of these devices is tested by a properly qualified security professional, in the same way you have a 'pen test' done on your Internet connection.

26

Phishing and its variations

- Phishing – fake e-mails designed to elicit information from an unsuspecting victim
- Indiscriminate 'bulk' phishing still being used, but increasingly we are seeing targeted 'spear phishing' attacks – much more carefully designed to attract responses from users of business networking sites.

27

Denial of Service

DDoS → "Distributed Denial of Service" Attack

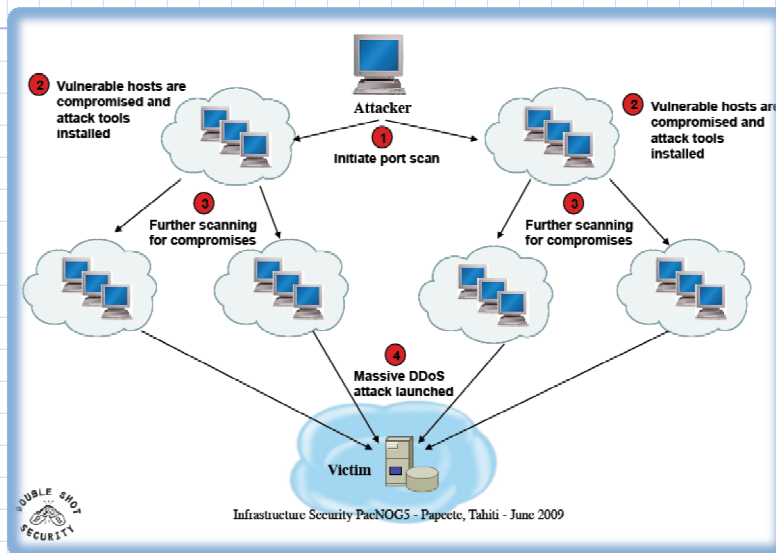
DOS → "Denial of Service" Attack

"A **denial-of-service attack (DoS attack)** or **distributed denial-of-service attack (DDoS attack)** is an attempt to make a computer resource unavailable to its intended users. It generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely."*

*http://en.wikipedia.org/wiki/DDoS#Distributed_attack

28

Denial of Service



Denial of Service - Countermeasures

- ◆ Ingress/Egress filters
- ◆ Capacity
- ◆ Contingency Response
- ◆ Firewalls
- ◆ Separation of services
- ◆ Monitor traffic flow
- ◆ Monitor services
- ◆ Monitor your logs

Denial of Service - Countermeasures

- ◆ Have a plan
- ◆ Know who to call
 - Do you have the technical contacts for your upstream provider?
 - Your technicians. Do you have a way to contact them during off-hours.
- ◆ Which services are critical. Can others be dropped? Turned off?
- ◆ Can you temporarily add capacity if necessary?

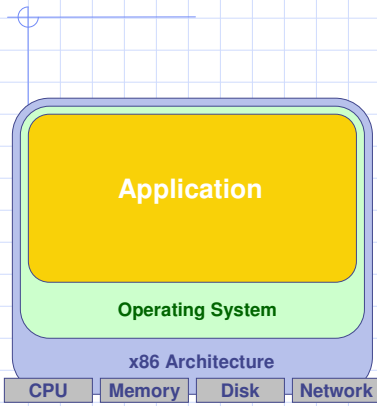
31

Introduction to Virtualization

- History of Virtualization
 - Mainframe origins
 - Computers in the 1990s & 2000s
 - Resulting IT challenges
- ⑩ What is Virtualization?
 - Key technology for today
 - Physical Server vs. Virtual Server
 - Virtualization layer
 - Virtual Machines

32

Traditional Physical Server

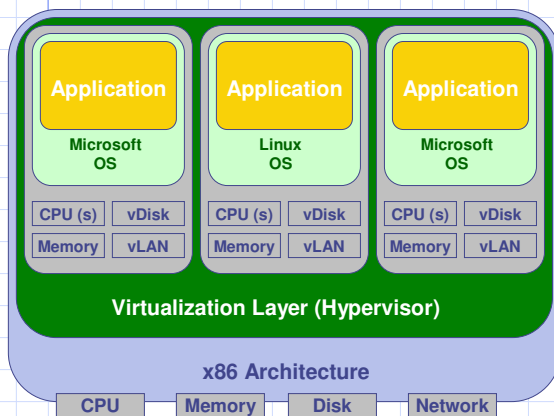


1 Physical Server, 1 Application

Traditional x86 Server Architecture

- Single operating system per machine
- Single application per machine
- Hardware components connected directly to operating system
 - ◆ CPU
 - ◆ Memory
 - ◆ Disk
 - ◆ Network Card

New Architecture: Virtual Server



3 Virtual Servers on 1 Physical Server

Virtualization Layer

- Addition of a virtualization layer called a "hypervisor"
- Several servers can be deployed as Virtual Machines (VM) on each physical box
- Each VM has its own operating system and application
- Can run multiple, different operating systems on the same machine
- If one VM fails, other VMs are unaffected

Why Virtualize?

- Consolidate Physical Resources
 - ◆ Logical resources may remain the same!
- Reduce Power Consumption
- Streamline System Recovery
- Simplify system maintenance
- Optimize Resource Utilization
- Testing and Development
- Training

35

Virtualization Security Benefits

- Application/service isolation
 - ◆ No more multi-purpose servers
- Improved system availability
 - ◆ HA possible for applications that do not natively support clustering
- Easy to create isolated sandboxes
- Easy to manage honeypots
- Improved security for mobile/remote users
 - ◆ Users connect with a clean system

36

Virtualization Risks

- VM sprawl – easy to create
- Rogue VMs – do you know how many you have/should have?
- Intensive consolidation can cause BC problems in a server failure
- An escaped VM may compromise the virtualization server
- 'Stale' snapshots and dormant VM's may have out-of-date AV and security settings, zombie accounts and may lack critical software patches.

37

Software Licensing in Virtualized environments

- Inconsistency amongst vendors
- Licensing approaches:
 - ◆ VM instance-based
 - ◆ VM hardware-based
 - ◆ Client connection-based
 - ◆ Physical hardware-based
 - ◆ Nonexistent
- Licensing management TCO may rise after a virtualization migration
- Variable metrics and physical hardware abstraction makes licensing compliance tracking difficult

38

Rimell Associates Ltd.

Web Infrastructure, Cloud Computing and SaaS

Rimell Associates

Definition

- "it is the access of data, software applications, and computer processing power through a 'cloud' of online resources"



4U

Software as a Service

- Processing and Data Storage are done externally to the firm on thin clients and accessed on a browser
- Turns software/hardware into a variable expense instead of a large fixed expenditure
- Enables firms to use only the resources they need on a very scalable basis

41

SaaS

- Software does not need to be owned by a company in order to use it. In fact, the firm's own tech support does not even need to be experts in the field of the software they are using.
- However large firms have very complex system requirements that can not be satisfied through a generic one-stop-shop software program. On top of that, they are relying on other firms to secure and maintain the integrity of their data.
- Since the industry is new and lacks regulation, there is a lot of resistance for firms to release their inner most secrets out into Clouds.

42

SaaS

- SaaS enables firms to access applications and databases, as well as conduct processes through any device. It is possible to do so because SaaS uses a web browser as the access point. Then virtual machines within the cloud do all the heavy lifting, leaving it only necessary to have a thin client to present the data back to the user.
- Essentially everything is done within the Cloud through SaaS, with the final results sent back to the users – thus eliminating any need for a firm to develop its own information system architecture.

43

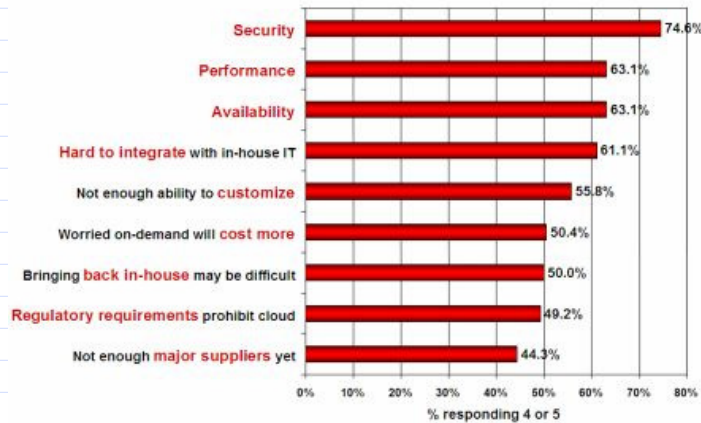
Benefits

- **Increased Storage**
Organizations can store more data than on private computer systems.
- **Allows IT to Shift Focus**
No longer having to worry about constant server updates and other issues, so can be more free to concentrate on innovation
- **Flexibility**
Cloud computing offers much more flexibility than past computing methods.
- **Highly Automated**
No longer do IT personnel need to worry about keeping software up to date.
- **Reduced Cost**
Cloud technology is paid incrementally, saving organizations money.
- **More Mobility**
Employees can access information wherever they are, rather than having to remain at their desks.

44

Security Is the Major Challenge

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Risks of Cloud Computing

- Privileged user access—what personnel within the service provider will have access to confidential data that is used in the cloud. What is the security protocol within the providers human resources system?
- IT Security Standards – There are multiple standards for security protocol for IT systems that have yet to be implemented into cloud computing.
- Regulatory compliance— the vendor will be required to participate in internal and external audits. They will need to find a way to accommodate auditors from all firms using their service.
- Data location—where will this data be stored? Does the user have any say?
- Data segregation—make sure that encryption is available at all stages and that these "encryption schemes were designed and tested by experienced professionals".
- Recovery— If there is a disaster what will happen to the data and will it be retrievable? Is the data always backed up in a separate location? How long will the system be down? .

Risks of Cloud Computing

- Investigative Support—inquires as to whether a vendor has the ability to investigate any inappropriate or illegal activity.
- Long-term viability— What will happen if the service provider goes out of business? What will happen to the data?
- Availability of Service – A very high bar has been set for service availability. When you go to google.com it is always working. Customers have become dependent on this reliability. It is very challenging to ensure this reliability for scalable software as usage quantity is hard to predict. If a surge in usage occurs, the system must be able to handle the surge.
- Data transfer bottlenecks – transferring large quantities of data can take a long time which may prove to be more expensive with pay-as-you go. For example, depending on the bandwidth speed, transferring terabytes of data could take days

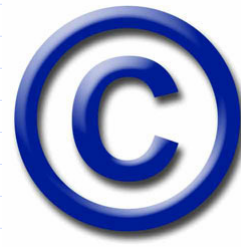
47

Rimell Associates Ltd.

Software Licensing Issues

Copyright Law

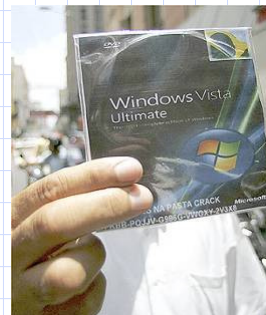
- ◆ Copyright gives legal protection to authors of materials so that they cannot be copied without the permission of the author or without financial compensation being given
 - Originally designed to protect books, photographs and sheet music it now applies to all work, no matter what format it is produced in e.g. video, music etc.
 - The **Copyright, Designs and Patents Act 1988** also makes the copying of software illegal.
 - This is the UK form of the **Intellectual Property Rights (IRP)** legislation which exists in most countries



49

Offences

- The Act exists to ensure people are rewarded for their endeavours by deterring illegal activity. It is illegal to do any of the following without permission
 - Copy software
 - Sell or distribute copies of software
 - Adapt software (cracking)
 - Transmit software



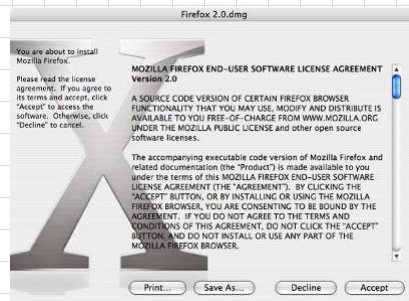
50

Penalties

- ◆ **FAST** (The Federation Against Software Theft) is an industry organisation that aims to prevent piracy by prosecuting anyone found guilty of breaching copyright law
- ◆ Penalties can include up to **two years** in prison and/or **unlimited fines**
- ◆ This applies to **organisations** as well as **individuals** e.g. if an employee is using software illegally on a organisation's computer the organisation can be held equally responsible in law

Software Licensing

- ◆ A software license agreement is a legal contract between the user and the software producer that sets out how the software may be used
 - When you purchase software you only get a **"licence to use"** you don't actually **"own"** the software
 - Standard licence allows you to put a single copy on one PC although some licences allow one other copy for **back up**



Common Licence Types

Multi user licence – s/w can only be installed on a fixed number of machines

Site licence – s/w can be used on all computers on one site e.g. a school or business

Academic licence - for students and teachers, usually single user



Licence by use – similar to a multi-user licence. s/w can be installed on many machines but only used by a fixed no. of people at any one time

53

Software Management /Licensing Audit Principles

- All software purchases should be centralised through a purchasing department or other designated company authority
- All software purchase requests should be in writing with department manager approval
- Ensure the software being requested is on the company's list of supported software
- Ensure that software has been purchased only from reputable, authorised resellers
- Ensure that on-line services and web applications are hosted with reputable Application Service Providers (ASPs), and that all relevant licenses and documentation from that ASP are available
- Ensure that original user materials (e.g., manuals, registration cards, etc.), licenses and receipts are preserved for each purchase;
- Ensure that employees do not buy software directly or charge it to their expense accounts
- Ensure that legal software cannot be downloaded from the internet by employees without special approval.

54

Software Management /Licensing Audit Principles

- Procedures should exist to identify desktop PCs, laptops or peripherals that are not being used
- Procedures should exist to identify outdated or unnecessary programs that can be deleted
- Procedures should exist to obtain the best possible prices through participating in volume licensing agreements
- Procedures should exist to ensure that volume license agreements are not violated by the installation of excessive numbers of copies
- Procedures should exist to identify unnecessary upgrades for unneeded software.

55

Software Management /Licensing Audit Principles

- The following information should be available for each copy of software installed on each computer:
 - Product name
 - Version
 - Vendor
 - Department owner
 - License type
 - Expiry date

56

Software Management /Licensing Audit Principles

- An inventory should exist of material related to software on corporate computers, including:
 - All disks, CDs, or other storage media used to install the programs
 - All original manuals and reference documentation;
 - All license documentation; and
 - All invoices, proofs of purchase, and other documents proving the legitimacy of the software. This includes invoices for computer systems that were sold with software pre-installed.

57

Software Management /Licensing Audit Principles

- A secure and storage area should exist for the following:
 - Original software CDs and disks
 - Licensing agreements
 - Warranties
 - Manuals
 - Invoices
 - Receipts or proof of purchase
- For open-source software, procedures should exist to ensure that the necessary license information is incorporated into any copies made under the terms of the license, and that any 'in-house' modifications made to the software preserve the rights of the original author(s).

58

Google hacking

- Using Google's amazingly comprehensive search facilities to dig out information that you didn't even know was on the Internet..

59

Google hacking

- Google's web spiders index just about everything they find
- Most of us use only Google's basic search facility with one or two keywords, but in fact there is an amazingly rich set of search operators available to us:

60

Advanced Operators

- cache:
 - define:
 - info:
 - intext:
 - intitle:
 - inurl:
 - link:
 - related:
 - stocks:
- filetype:
numrange 1973..2005
source:
phonebook:

61

SiteDigger 2.0

- **<http://tinyurl.com/28aeh>**
- The tool requires Google web services API license key.
 - Your license key provides you access to the Google Web APIs service and entitles you to 1,000 queries per day.

10 System Requirements

Windows .NET Framework (can be installed using Windows Update)

62

Who's got an Oracle database?



site:edu inurl:isqlplus

Search [Adv](#)

Search: the web pages from the UK

Web [+ Show options...](#)

[iSQL*Plus Release 10.2.0.1.0 Production](#)

Unauthorized use of this site is prohibited and may be subject to civil and criminal prosecution. *
Indicates required field ...

[dbserv.eis.gvsu.edu:5560/isqlplus/ - Cached](#)

[iSQL*Plus Release 9.2.0.8.0 Production: Login](#)

iSQL*Plus logo. Help. Login. Username: Password: Connection Identifier: DVOLUSER, DVOLEXP.

[web2.dal.devry.edu/isqlplus/ - Cached - Similar](#)

63

Connected...



Login

Username:

Password:

Connection Identifier:

Login

Notice they've already given us a connection ID –
Now I need a valid username and password – where
did I put that copy of dpl.htm?

64

Protecting yourself...

- Consider removing your site from Google's index.
<http://www.google.com/remove.html>
- Make sure all of your 'default' accounts have been secured.
- Examine your system logs regularly to detect suspicious activity.

65

Robots.txt

- **Use a robots.txt file.** Web crawlers are supposed to follow the robots exclusion standard.
- This standard outlines the procedure for "politely requesting" that web crawlers ignore all or part of your web site.
- This file is only a suggestion. The major search engine's crawlers honor this file and its contents.
- For examples and suggestions for using a robots.txt file, see <http://www.robotstxt.org>.

66

Example Robots.txt

- User-agent: *
 - Disallow: /images/
 - Disallow: /stats/
 - Disallow: /logs/
 - Disallow: /admin/
 - Disallow: /comment/
 - User-agent: Googlebot
 - Allow:
 - User-agent: BecomeBot
 - Disallow:
 - Disallow: /
 - Disallow: *
 - User-agent: MSNBot
 - Disallow:
 - Disallow: /
 - Disallow: *
- By default tells others to not scan specific paths
Allows Google to scan
Tells BecomeBot and MSNBot to go away entirely.
Place the robots.txt in the root of your HTML documents directory.
- See also
Removing Your Materials from Google
How to remove your content from Google's various web properties.
<http://hacks.oreilly.com/pub/h/220>
- Robots.txt generator
<http://tinyurl.com/7pc4k>

67

Network perimeter security

- Do you know what's on your network?
 - Connection of unauthorised devices is a serious risk:
 - In a survey of 987 end-users and 204 CIOs and IT directors across Western Europe, 95 per cent said that they had used at least one consumer device that they have purchased themselves for work purposes. In the UK, 38 per cent of 'i-workers' use smartphones for work, although only 14 per cent of the employers surveyed believed this to be the case.
Source: Secure Computing 6/7/2010
- 10 How many of these devices are attached to your network, and what are they doing?

68

The Ten Commandments of Network Security - 1

- Know where your network begins and ends, e.g.
 - ◆ A network's physical boundaries can be a lot wider than you think
 - What about cabling to areas used by the public? - interview rooms libraries, community rooms, art centres etc.
 - If you are in a shared building, does anyone else use the same cabling?
 - Rogue wireless points can extend your network – sometimes users set them up because they can't wait for conventional cabling to be installed - what's their range?
 - Have internal LAN users made unauthorised connections to the Internet, and how would you know?
 - Does your Windows domain trust any others?

69

The Ten Commandments of Network Security - 2

- Physically secure your infrastructure devices
 - Make sure that switches, hubs, routers etc are locked away in secure cabinets – they have a serial port on the back allowing anyone to plug in a laptop and reconfigure them.
 - Watch out for cable tapping if you are concerned about the physical route your data will take.
 - Can IT account for all the infrastructure devices completely and accurately?

70

The Ten Commandments of Network Security - 3

- Logically secure your infrastructure devices
 - Many network devices are 'managed' – i.e. they can be remote controlled via the network and all have default passwords/ID/access codes – make sure they have all been changed.
 - Ensure that the two SNMP community names 'public' and 'private' have been changed, and that SNMP-capable devices will respond only to designated workstations.
 - Enable logging on network devices that are capable of doing so, and send the logs to a central point for inspection.

71

The Ten Commandments of Network Security - 4

- Don't use insecure remote access methods for network devices
 - Programs such as Telnet use clear-text authentication to log on – use SSH instead wherever possible
 - Lots of network devices have a built-in web server for admin – do you really need it?
 - Use Terminal Services for Windows remote admin, not less secure alternatives such as VNC
 - Change the device passwords occasionally!

72

The Ten Commandments of Network Security - 4

- Save all configuration files
 - All network infrastructure devices have a basic configuration supplied by the manufacturer, that usually has to be changed. If the device is replaced or has to be repaired, it will revert to its original factory configuration.
 - Make sure that the network administrators have saved a copy of the current system configuration for every critical network device, and that they are able to restore it.

73

The Ten Commandments of Network Security - 5

- Consider implementing measures to prevent or detect the attachment of unauthorised workstations or laptops.
 - Most networks use DHCP and will therefore hand out an address to any requesting device
 - Ensure that network connection points in unused areas are disabled or disconnected.
 - Use 'port locking' or 802.1x security in high-risk environments to prevent unauthorised devices being able to use network ports at all.
 - Review the allocation of DHCP addresses and try to account for them

74

The Ten Commandments of Network Security - 6

- Don't run unnecessary network services
 - Many network devices and most operating systems run network services that are not necessary for business purposes (did you really intend that W2K server to be a Web server as well?)
 - Scan servers and network infrastructure devices, and find out why each service is running – disable any that cannot be justified for business reasons

75

The Ten Commandments of Network Security - 6

- Keep device firmware up to date
 - We're all used to Windows update offering to keep our Windows 2K/XP/Vista/Win7 workstations and servers up to date, but remember that infrastructure devices also have 'mini' operating systems inside them (e.g. Cisco's IOS), and these have had their share of bugs and security exposures.
 - Check that a system exists for learning about new security threats, and deploying security fixes.

76

The Ten Commandments of Network Security - 7

- Make all of your external access connections (inbound and outbound) through a firewall
 - Who needs to access your network from outside?
 - ◆ Teleworkers?
 - ◆ Software support companies?
 - ◆ People just needing to check their e-mail?
 - ◆ Roving sales reps?
 - Is it possible to bring them all in through one route (the firewall) and dispense with the plethora of dial-in and ISDN connections to your servers etc?
 - WLAN devices should always be treated as untrusted – never attach them to the inside of the LAN, always connect them via an firewall and/or VPN

77

The Ten Commandments of Network Security - 8

- Install a capable firewall and Intruder Detection system, and configure them correctly
 - Get a firewall from a reputable supplier (Cisco, Nokia/Checkpoint, GTA)
 - Ensure that its static configuration is checked immediately after installation, before going live
 - Have a security assessment/penetration test performed:
 - At least every 12 months
 - After any significant upgrade

78

The Ten Commandments of Network Security - 9

- Review the security of networked applications
 - Modern firewalls, properly configured, are very effective – therefore the hacker will try to exploit the only two things that can pass legitimately through your firewall – web traffic and e-mail.
 - ♦ Use a quality e-mail scanner and anti-virus package
 - ♦ Use a web proxy/web page scanner to control/monitor user's access to the web
 - ♦ Check for the presence of exploitable vulnerabilities in your internet-facing applications (e.g. SQL injection)
 - ♦ Make sure your security testers perform a proper check, and that they include application vulnerability tests as well as the standard network tests.

79

The Ten Commandments of Network Security - 10

- Education, education, education....
 - A lot of network compromises are the result of ignorance:
 - ♦ Make people aware of your security policy
 - ♦ Educate them about fake web sites, e-mail 'phishing' attacks etc.
 - ♦ Subscribe to security sites like SANS to get the latest info
 - ♦ Keep network security tools up to date and deploy them regularly

80