Global Information Assurance Certification Paper

SECURING THE HOME NETWORK

GSEC Practical v1.4b Option 2

ABSTRACT

This paper describes the securing of two components of a small home network using Information Assurance (IA) principles to guide the process. The intention is to provide home users and small businesses with some insight as to how IA can be applied successfully to the small office or home network environment. The paper first identifies what risks face the network then addresses each one with some form of control.

INTRODUCTION

Whilst Information Security is of particular concern in the corporate environment, workers who perform duties from home often do not address it. Users write up sensitive company documents on personal laptops, administrators control corporate systems from the same computer on which Internet games are played and un-trusted files downloaded from the Internet. This paper addresses two components of a home network with an aim to improve basic computer security and provide some level of assurance. The network is used for a number of purposes, as described in the Existing Network section of this document.

SCOPE

This paper will cover the securing of a host that provides services to the Internet (WWW and SMTP hosting), and securing a desktop host from compromise. It will not be covering any of the internal hosts that only provide local services (File server, DNS Server, DHCP Server) or hardware configuration. We will not be taking a detailed look at the firewall, however we will mention what rules need to be applied by it when there are security implications.

EXISTING NETWORK

The network is shown below in Figure 1. Internet access is provided via a 256Kbps Microwave link to the ISP. A single public IP address is provided for use, whilst all machines on the LAN use private addressing. The network is used for the usual personal Internet use (browsing, e-mail, computer games), as well as mail and web hosting.

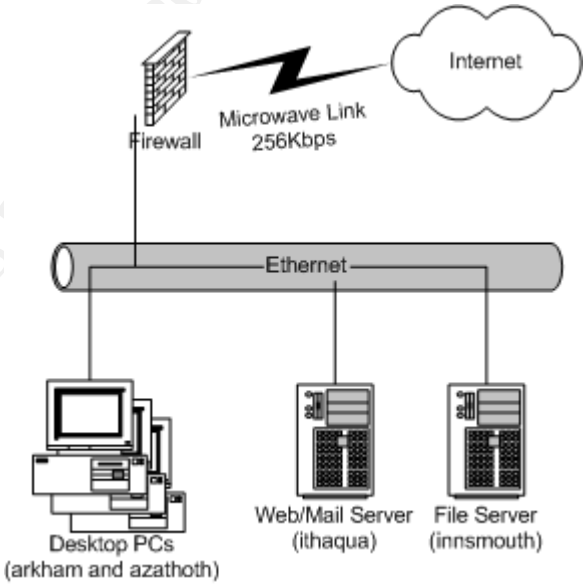


Figure 1

The following table summarises each machine on the network, and what function

they perform.

Host	OS	Purpose
gateway	Dachstein LEAF	Firewall
innsmouth	Debian GNU/Linux 3.0	Fileserver
ithaqua	Trustix Linux	Web/Mail server
dromos	SunOS 2.6	DNS/DHCP server
various	Windows	Desktop PCs

RISKY BUSINESS

The first step is to examine the risks that are present in relation to the system. To do so, a discussion was held amongst the users. Firstly the assets (What is it we want to protect), threats and vulnerabilities were identified and then the impact and the level of risk to each:

Asset	Threat	Vulnerability	Impact	Rating
Personal Information (Credit card numbers, Internet Banking details)	Internet based attackers	Fraudulent use of information	Loss of money Loss of reputation	HIGH
Web site	Internet based attackers	Web site defacement, used for attacking third party systems or other local systems	Loss of reputation, loss of data, loss of service	HIGH
Remote Management of Employer Systems	Internet based attackers	Compromise of sensitive commercial information	Loss of money Loss of reputation Loss of job	VERY HIGH
Mail content	Internet based attackers	Compromise of personal information	Loss of privacy	LOW

Next, we will look at the systems on the network, and see what risks are involved in each system, and then discuss the controls that will be applied to each.

Internet Server

Attack against the Web/Mail server is the highest risk the network faces.

According to Internet Security systems Q2 2003 *Internet Risk Summary* [1], 45.54% of attacks are aimed at port 80 (HTTP), whilst port 25 (SMTP) accounts for 3.37%. Whilst HTTP has decreased from 96% in the last 18 months, it is still the most likely vector for attack. The impact of this server being breached is high, as not only is there a possible loss of Integrity (Website Defacement) and Availability (Denial of Service), there are currently no security controls between the Desktop machines, and a breach in the security of the server could lead to a loss of Confidentiality (personal information).

User Desktop

The desktops have the most sensitive information on the network: They are used for Internet Banking, online shopping, gaming, web-browsing, e-mail and remote administration of sensitive commercial networks. Possible vectors include viruses, hybrid threats and Trojans. One impact of an attack on the Desktops is quite high, since loss of the information could result in financial loss to both the users, and the user's employers. Attacks specifically directed at the user's organisation (called a Targeted Attack) are of particular concern, however according to statistics gathered by the Computer Research Crime Center (CCRC) [2], they are unlikely. Typically, Targeted Attacks are directed against large corporate networks rather than home connections.

IDENTIFYING SECURITY CONTROLS

To reduce the high risks faced by the identified components of this system, controls must be put in place to lower, mitigate or transfer the risk.

The steps taken to apply security should clearly link back to the assessed risks. As such, this section will be broken down by the risks that the system faces. The steps that have already been taken, and the additional controls that will be required, will be identified.

Server

The overall risk in this area can be reduced through a number of methods. Firstly, we will reduce the impact of the server being compromised by moving it into a second, less trusted, network segment behind a firewall. This will reduce the access the server has to the Internal network, thus making it more difficult to exploit the Clients from the Server. Secondly, we will review the network footprint of the server, and remove any non-required services. This will reduce the possible vectors of attack, and reduce the number of software packages that will need to be kept up to date.

Clients

Access to the Desktops from the Internet is currently disallowed by the firewall. Anti-virus software runs on some, but not all, clients. The risks in this area are more difficult to address, as functionality is at a premium. We will reduce these risks by two methods: Removing unnecessary services from the Desktops to reduce possible attack vectors, and installing Outpost Free Personal Firewall [3]

to provide a second layer of network filtering, to mitigate network based attacks. The existing Anti-Virus software combined with the Personal Firewall will be sufficient to reduce the overall level of risk to the Desktops. Anti-Virus software will be installed where required.

As an additional point, some amount of User Education will be required to ensure that the measures taken in this section are used. Ultimately, it is the user who decides whether security controls are used; there are ways to subvert most technical controls.

IMPLEMENTING THE CHANGES

Implementation will be done in phases, addressing first the server, and then the clients. Ideally these changes would be made to freshly installed systems

Securing the web server

The following steps were performed to secure the web server.

1. Analyse the network profile of the server

In order to ascertain what services were running and available on the server, nmap [4] was used to determine the network profile. We could have used the native utility netstat to do so, however to ensure an accurate portrait of the network footprint was painted, it was necessary to use a network based tool. First, a TCP port scan[1] was performed.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on ithaqua (192.168.1.3):
(The 1594 ports scanned but not shown below are in state: filtered)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
80/tcp     open        http
139/tcp    open        netbios-ssn
143/tcp    open        imap2
901/tcp    open        samba-swat
3306/tcp   open        mysql
Remote operating system guess: Linux 2.1.19 - 2.2.20
Uptime 101.001 days (since Sat Apr 12 16:37:18 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 406 seconds
```

Next a UDP port scan[2] was performed.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on ithaqua (192.168.1.3):
(The 1466 ports scanned but not shown below are in state: closed)
```

[1] The command used was 'nmap –sT –PT –P1 –O –T3'

[2] The command used was 'nmap -sU -PT -PI -O -T 3'

```
Port       State       Service
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 1496 seconds
```

SSH is used to manage the server remotely, so will need to be left open. SMTP is used for mail delivery and http is used for web content, both of which are legitimate services. Mail clients on the internal network use IMAP2.

137/udp, 138/udp and 139/tcp are all NetBIOS ports, part of the Samba package. Samba provides a UNIX implementation of Server Message Block (SMB), the common Windows filesharing protocol. Samba-swat is SWAT (Samba Web Administration Tool). Both Samba and SWAT can be removed, as they are not essential services. Port 3306/tcp is the MySQL Database server. No remote hosts access this service remotely, so it can be closed.

2. Harden the server by removing unnecessary services

The host operating systems package management tools were used to remove unnecessary packages, in this case the Redhat Package Manager (RPM).

```
rpm –e samba
```

SWAT is started by Inetd and its entry is not removed by RPM, so it must be manually removed from the configuration file /etc/inetd.conf.

```
# The swat daemon (needs samba):
#swat      stream  tcp     nowait.400      root /usr/sbin/swat swat
```

MySQL has the option of turning off remote access. Since only local web content accesses the database server, this was used. The '—skip-networking' option was entered into the startup scripts '/etc/init.d/mysql' to effect this change.

```
$bindir/safe_mysqld --skip-networking --datadir=$datadir --pid-
file=$pid_file >& /dev/null &
```

Another run of nmap shows that those services are now closed off.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on ithaqua (192.168.1.3):
(The 1597 ports scanned but not shown below are in state: filtered)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
80/tcp     open        http
143/tcp    open        imap2
Remote operating system guess: Linux 2.1.19 - 2.2.20
Uptime 101.224 days (since Sat Apr 12 16:37:20 2003)
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 407 seconds
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1468 scanned ports on ithaqua (192.168.1.3) are: closed
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 1469 seconds
```

As shown above, only those ports necessary for the operation of the system are now listening.

3. Create a DMZ Segment on the Firewall and move the server

The Firewall currently runs LEAF (Linux Embedded Application Firewall) Dachstein, a single floppy distribution of Linux with modular functionality. The system is designed with a DMZ segment in mind, and up until now it hasn't been used. We need to enable this functionality, and configure the firewall to apply the following logical filters. According to *Internet Firewalls and Network Security* [5] the following:

- ALLOW any protocol FROM Internal network TO DMZ
- ALLOW any protocol FROM Internal network TO Internet
- ALLOW http FROM Internet TO server
- ALLOW smtp FROM Internet TO server
- ALLOW smtp FROM server TO Internet
- DENY anything not already specified

Here are the appropriate entries in the firewall ruleset after the DMZ segment has been added (Slightly edited for brevity).

```
                    Chain input (policy DENY: 0 packets, 0 bytes):
target prot tosa tosx ifname source          dest             ports
                                      ...
ACCEPT tcp  0xFF 0x00 eth0   0.0.0.0/0     XXX.XX.XXX.210 * ->   80
ACCEPT tcp  0xFF 0x00 eth0   0.0.0.0/0     XXX.XX.XXX.210 * ->   25
                   Chain forward (policy DENY: 0 packets, 0 bytes):
target prot tosa tosx ifname source          dest             ports
                                      ...
MASQ   tcp  0xFF 0x00 *      192.168.2.1   0.0.0.0/0        80 ->   *
MASQ   tcp  0xFF 0x00 *      192.168.2.1   0.0.0.0/0        25 ->   *
                                Port Forwarding
prot localaddr       rediraddr              lport    rport  pcnt  pref
                                      ...
TCP  210.54.175.210  192.168.2.1              25       25    10    10
TCP  210.54.175.210  192.168.2.1              80       80    10    10
```

Now that the firewall has been set up, we can move the server into the DMZ segment. We change the IP address and default gateway of the server, and then physically connect it to the new segment.

Securing the Desktop

The following steps were followed to secure the desktop. These steps were performed on one desktop, azathoth, as a proof of concept.

1. Analyse the network footprint of the Desktop

As with the Server, the network profile of the system in question can be determined through the use of nmap.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on azathoth (192.168.1.11):
(The 1596 ports scanned but not shown below are in state: filtered)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
5000/tcp   open        UPnP
Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP
Nmap run completed -- 1 IP address (1 host up) scanned in 414 seconds
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on azathoth (192.168.1.11):
(The 1459 ports scanned but not shown below are in state: closed)
Port       State       Service
123/udp    open        ntp
135/udp    open        loc-srv
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
445/udp    open        microsoft-ds
500/udp    open        isakmp
1030/udp   open        iad1
1110/udp   open        nfsd-keepalive
1900/udp   open        UPnP
Too many fingerprints match this host for me to give an accurate OS
guess
Nmap run completed -- 1 IP address (1 host up) scanned in 18 seconds
```

Obviously, there's a lot of work to do here! This default WinXP SP1 install provides a large amount of network services. 137/UDP, 138/UDP and 139/TCP are all NetBIOS. 445/udp and 445/tcp are both CIFS-over-TCP, an implementation of the SMB protocol directly over TCP rather than through the NetBIOS layer.

2. Remove unnecessary services

Filesharing between the Desktops is still required on this network, so the NetBIOS ports will be left open on these hosts. According to *Minimising Network Services on Windows* [6] IPSec, SSDP and Windows Time can be easily stopped using the 'net' command.

```
C:\Documents and Settings\User>net stop policyagent
The IPSEC Services service is stopping.
The IPSEC Services service was stopped successfully.
```

To ensure that these services do not start again, we disable them with the 'sc' tool, as described by Marchand.

```
C:\Documents and Settings\User>sc config policyagent start= disabled
[SC] ChangeServiceConfig SUCCESS
```

Next, rpcdump from the RPC Tools collection [7] was used to find what RPC services were running. rpcdump connects to host and enumerates the resources being made available via RPC on that host.

```
C:\Documents and Settings\User>rpcdump azathoth
```

The output from this tool is quite comprehensive, however some digging found the following two entries.

```
IfId: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc version 1.0
Annotation: Messenger Service
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncacn_ip_tcp:192.168.1.11[1025]


IfId: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc version 1.0
Annotation: Messenger Service
UUID: 00000000-0000-0000-0000-000000000000
Binding: ncadg_ip_udp:192.168.1.11[1027]
```

The bold text above indicates the ports that have been identified. Internet spammers have recently targeted the Messenger Service for use in unsolicited advertising [8]. Though it is filtered at the firewall, the service is not needed on the desktop, so can be disabled as above. On doing this and rebooting the system port 1025 was found to till be open. It shows up in rpcdump, but has no service associated with it. Marchand points out in his guide that the Task Scheduler service also holds open a port. Disabling the Task Scheduler and rebooting closed the unnamed port. However, some time after rebooting, several high ports were opened, and it is not apparent as to what caused this to happen. Another run of rpcdump showed several ports being held open by unnamed processes and services. As the intention in this section is not to fully secure the workstation, but minimise the amount of access allowed, I have not followed up

on these additional ports. However, we also shut down the dnscache, as suggested by Marchand.

2. Install personal firewall

In order to give us greater 'defence in depth' we will install Outpost personal firewall.

We installed the software on a Windows XP desktop. The installation was uneventful, with the usual slew of prompts and buttons. After a restart and going through an Auto-update sequence, the firewall was active. It began to pop up dialog boxes prompting me into action about network events.

Figure 2

The software has a number of different modes it can operate in, similar to Internet Explorer's trust levels.

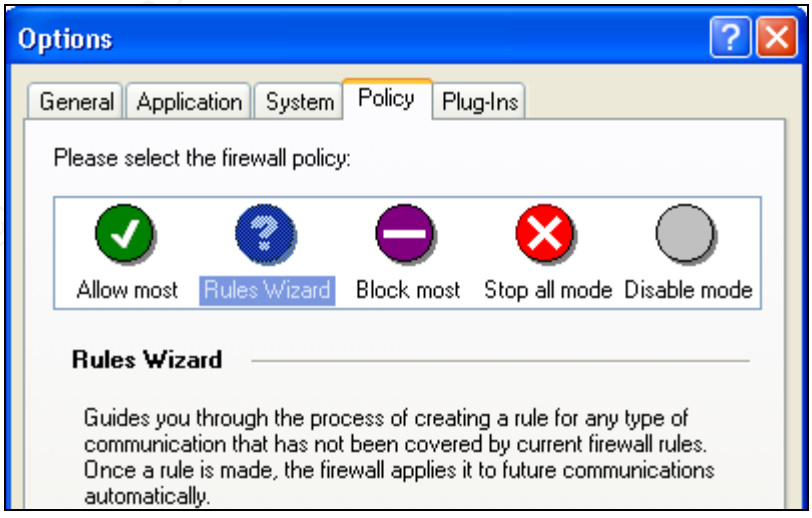


Figure 3

By default, the application runs in 'Rules Wizard' mode, which will prompt each time a new network connection opens up. The vendor recommends that new users run in this mode for several days at least, to get an accurate profile of what traffic flows over the network.

To test the effectiveness of Outpost, nmap was again run against the desktop from a locally connected system, since if the desktop firewall were to rebuke an attack then gateway, the internet firewall, is probably already compromised. Initially, nmap would try to ping the host in question before commencing the scan, which failed because the firewall was rejecting the packets. To avoid this the –p0 flag had to be used to prevent any ping attempts.

TCP Scan

```
# nmap -sT -P0 -O -T 4 192.168.1.11

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on azathoth.miskatonic.ac.nz (192.168.1.11):
(The 1597 ports scanned but not shown below are in state: filtered)
Port       State       Service
135/tcp    open        loc-srv
137/tcp    closed      netbios-ns
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
Remote operating system guess: Windows 2000/XP/ME

Nmap run completed -- 1 IP address (1 host up) scanned in 277 seconds
```

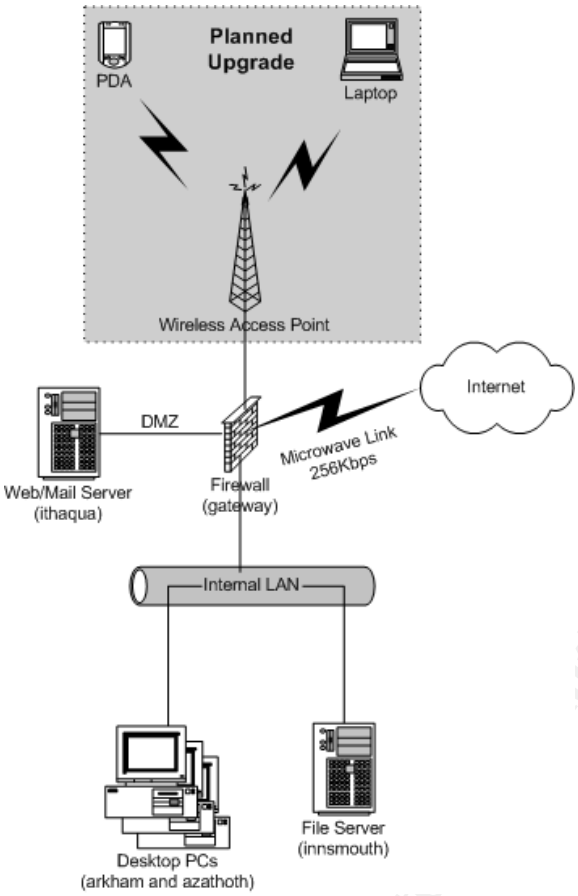
UDP Scan

```
# nmap -sU -P0  -F -O -T 4 192.168.1.11

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Skipping host  azathoth.miskatonic.ac.nz (192.168.1.11) due to host
timeout

Nmap run completed -- 1 IP address (1 host up) scanned in 352 seconds
```

These results indicate that only the firewall is allowing access to the NetBIOS ports, and CIFS-over-TCP, however it appears that it is dropping unsolicited UDP ports, since nmap timed out on the UDP scan. Port 137/tcp is in a closed state, which indicates that the firewall is allowing the connection through, however the desktop isn't actually listening on that port. It is surmised then that in a default configuration, Outpost does provide *some* protection.

POST-OP NETWORK

After the changes were made to the system, we reviewed the process. Firstly, a risk analysis was performed and controls were put in place to mitigate those risks. These controls were:



1. Move Internet accessible services to a separate physical segment
2. Reduce the number of services offered by the web server
3. Reduce the number of services offered by the clients
4. Install a personal firewall to provide control over applications connecting to the Internet.

These controls do provide additional security however vulnerabilities still exist. The risk analysis performed on the system was somewhat informal, and the low value of the target meant that controls also needed to be low value.

These controls provide a number of gains and also present a number of restrictions on the systems functionality. We analysed these to see what impact the changes had, both good and bad.

Gains

1) Limited damage when server gets compromised due to DMZ structure. Lower risk of Internal hosts being compromised from the server.
2) Fewer services running on the server and the desktops means less potential entries into the system.
3) Personal Firewall means even if the Internet firewall is compromised, there is a layer of protection between the client and the attacker.

Restrictions

1) Higher desktop security now limits the functionality provided to the user.
2) Removing Samba from the server meant more difficultly is involved in getting web content loaded on the server. Some replacement would be required.

Overall, it was concluded that the benefits gained through the implementation of these controls outweighed the problems, and with a little more work the

restrictions could be overcome.

It is surprising how many services were being offered by the Windows XP desktop. When this was shown to another user, there was interest in installing Personal Firewall/Anti-virus software on other PCs. So it seems the users are interested in having the peace of mind that good security can bring.

REFERENCES

1. Internet Security Systems, “Internet Risk Summary for April1, 2003 through June 30, 2003”,
   URL: https://gtoc.iss.net/documents/summaryreport.pdf (22 July 2003)
2. Richmond, Riva “Internet Hacker Activity Increases”, Yahoo! Singapore Finance, 5 February 2003,
   URL: http://sg.biz.yahoo.com/030205/72/372p0.html (22 July 2003)
3. Outpost Free Personal Firewall
   URL: http://www.agnitum.com (22 July 2003)
4. NMAP v3.0.0
   URL: http://www.insecure.org/nmap/nmap_download.html (22 July 2003)
5. Siyan & Hare, Karanjit & Chris Internet Firewalls and Network Security. Indianapolis: New Riders Publishing, 1995. 176 – 184
6. Marchand, Jean-Baptiste “Minimising Windows Network Services”, 2 September 2002,
   URL: http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html (22 July 2003)
7. RPC Tools v1.0
   URL: http://razor.bindview.com/tools/desc/rpctools1.0-readme.html (22 July 2003)
8. CIAC, “CIACTech03-001: Spamming using the Windows Messenger Service”, 29 October 2002,
   URL: http://www.ciac.org/ciac/techbull/CIACTech03-001.shtml (22 July 2003)