Global Information Assurance Certification Paper

Using OpenBSD To Secure A Home Networking Environment

Security Essentials GSEC Practical Version 1.4b

Nick Besant, July 2003

Abstract

Domestic usage of network enabled hardware is rapidly increasing as technology advances and price decreases, together with low-cost always-on bandwidth, encourage the home user to connect more than just a single home computer to the internet. With ever-decreasing costs for connections such as ADSL and cable, and retail computer outlets promoting home networking kits, users are able to share connectivity between multiple home computers, portable devices such as laptops and PDAs, gaming consoles and now even domestic white goods. Major console manufacturers provide Ethernet connectivity options for their devices, and PVRs (digital recording devices for live television) and some media systems are also network ready. For the gadget lover, white goods such as refrigerators can come with interactivity and networking.

1. Introduction

Given the quantity and breadth of network ready devices that are available, it can be difficult to control security for every device within the home; desktop or server machines will require operating system and application patches, other users (such as children) may desire to use services such as chat and instant messaging, and gaming devices require access to internet servers. Providing a firewall to protect the house network is only the first step towards gaining sufficient security; such considerations as bandwidth usage, types of traffic and content filtering must also be taken into account. Home workers may require unfettered access to connect to corporate networks for services other than web traffic, PVR devices may need to receive multicast traffic, and other devices will have separate requirements.

Home networks are unique in that there are no usage policies, liability clauses or defined service level agreements, and rarely carry sensitive or valuable traffic, which means equipment is usually connected and maintained in a haphazard fashion. Combined with this and the sizeable bandwidth available to the home market now, these devices present an ideal target for a casual system cracker; they are less likely to be targeted by a professional attacker due to a lower likelihood of valuable information being available, but present a large surface area on which to launch scripted attacks.

The aim of this paper is to identify the inherent risks in such a network, and discuss and implement best practices to provide an acceptable level of

security, using the OpenBSD operating system to provide support and security services such as firewalling, email and web filtering and web proxying. Issues such as provisioning bandwidth to specific groups or users will also be discussed, together with basic intrusion detection and notification capabilities and dealing with unexpected requirements such as gaming parties and provision of connectivity to others - such as neighbours. This paper is aimed at the requirements for a family of five, with each requiring individual access as well as shared devices, with an existing network environment, which will be based on a connection package offered by a popular UK ADSL provider to provide a frame of reference.

2. Overview of devices and their requirements

The following list presents a representation of typical devices likely to be present within a home environment, together with their requirements for access and bandwidth usage, as well as priority of network traffic. For the purposes of this paper, bandwidth requirements will be classed as follows;

- Class 1 : Low (not sustained)
- Class 2 : Medium with bursted traffic (not sustained, occasional bursts)
- Class 3 : High (sustained and or constant bursts)

Note that these are based on observed traffic from both a home and a corporate environment for several traffic types, and as such are only a basic guideline, and as such do not reflect any quantative measurements..

2.1 Corporate laptop

Staff working from home or with portable devices have an increasing need and capability to work remotely. This kind of device will usually be subject to a corporate security policy, although this may only cover anti-virus and desktop settings.

Typical usage includes web browsing – covering mail access, company portals or extranets and general research or browsing. Requirements can also exist for VPN connections back to the corporate firewall; some implementations of which can cause issues with NAT (Network Address Translation).

This paper will assume the remote worker is using a Checkpoint VPN to access their corporate network in addition to internet traffic direct from the machine. This puts the machine into Class 2, as bandwidth is consumed for sustaining the encrypted tunnel and also for local web and email traffic. This is also assumed to be a Microsoft Windows XP machine.

2.2 Home Server

This class of machine provides shared resources such as data or music files for the users within the household as well as providing public-facing services such as email and DNS. It will be classified as a Class 1 device, as external bandwidth is required only for sending and receiving email and DNS lookups. It is assumed this will run OpenBSD.

2.3 Home Desktop

This category of machine provides access for family members to local resources, internet, email and other services such as chat and file sharing. It is assumed there are four of these devices, running either Microsoft Windows XP or Redhat Linux 9. Each device is classified as Class 2 due to the nature of the services in use together with irregular traffic needs such as file downloads.

2.4 Gaming Console

This machine provides access for group-play games using a standard gaming console, and making a connection to a shared public internet server. This is a Class 2 device as constant game state information is sent during use. Note that this is not a permanently connected device, and is likely to require bandwidth during peak periods at home (evenings and weekends).

2.4 Web Desktop

This category of machine provides shared access from a common point within the house such as the family room or kitchen. Its primary use is for light internet access, and is classified as a Class 1 device.

2.5 Assumptions

It is assumed that all 8 of the above devices are regularly connected to the home network, with occasional requirements for additional devices in any of the categories.

3. Risk analysis and mitigating factors

Each device that will be connected to the network has several risks associated with it. These range from potential virus and worm infections to remote compromise, as well as misuse by household members. Due to the always-on nature of the internet connection in use, this network presents a higher risk of attack than a simple analogue dial-up connection. (CERT, http://www.cert.org/tech_tips/home_networks.html, Dec 2001)

3.1 Corporate Laptop

For the purposes of this paper it will be assumed that the corporate laptop is subject to a corporate security policy and as such has been security hardened, is kept up to date with patches and runs a virus scanner.

3.2 Home server

Given the budget for a home network is likely to be small, it is unlikely that a central file sharing / repository service and email and DNS can reside on separate hardware devices. This presents a risk in that the same machine will store possibly confidential files meant only to be accessed from the private network, and will also need to be on the public internet to provide DNS externally and send and receive mail. This risk will be mitigated to some extent by providing port forwarding services on the firewall, so the home server will not be directly connected with a public IP address.

3.3 Home Desktop

These devices are likely to provide the highest security risk as they are likely to be required to connect to public services such as chat, instant messenger, and a variety of web pages. As these are likely to be used by children as well as adults, the machines themselves cannot be locked down any further than is required as users will need to be able to install games, connect to online services and communicate with friends. Risk can be reduced through appropriate firewall and security policies, as well as regular scans.

3.4 Gaming Console

Due to the relatively recent adoption of broadband console gaming services in Europe, only a small amount of risks are associated so far with these devices, although it is likely that these machines may be used in future for distributed attack purposes. Possible risks can include information disclosure and system compromise, although the danger is low as little or no personal information is stored within the device and data loss is likely to involve gaming information only. (Alex Sands, Security Focus http://www.securityfocus.com/news/490, June 19 2002)

3.5 Web desktop

This type of machine can be restricted to only allow web and file server access (to allow users to save resources). This provides additional security as the machine need run few services and only a browser. Provided the browser and related technology are kept up to date this machine should stay secure.

4. Usability versus security

As this is a home environment, security must be as transparent as possible. Home users are unlikely to be happy to remember several long and complex passwords or access procedures – a compromise must be found between usability and security (Brian R. Krause, Usability : A Requirement for

Security, http://www.encentuate.com/perspectives/usability.htm, Date unknown). This also applies to access rules through the firewall; good practice is to explicitly block outbound connections rather than allow all, however a home administrator may need to perform regular changes to rule bases to allow access to alternate services such as chat, P2P networks and FTP services.

Family relationships are likely to restrict usual enforcement of security practices (such as disciplinary procedures), and family members are unlikely to be motivated to care about security – making the users themselves the weaker link in the chain. This means that users must be able to work and play with a minimal direct level of interaction with the security mechanisms (Alma Whitten and J. D. Tygar, Usability of Security : A case study, http://secinf.net/cryptography/Usability_of_Security_A_Case_Study.html , December 18, 1998)

To achieve this, the network perimeter and the internal machines must be protected and regularly maintained with regular rule checks and patching, while allowing for occasional access for untrusted devices (such as devices present for testing, children's friends, new consoles etc.) by providing a restricted segment (such as a DMZ).

Taking the above into consideration, the border device (ADSL router / set top box) should act as a bridge device to lower the likelihood of directed attacks – this allows the initial stage of access restriction to happen on a trusted machine. Outgoing web access will pass through this machine, and is likely to be to similar sites, so bandwidth consumption can be reduced (and filtering introduced if required) by using a proxy server (such as Squid - http://www.squid-cache.org/) in a transparent caching mode (Daniel Hartmeier, Transparent Squid, http://www.benzedrine.cx/transquid.html, Date unknown (rev. 22 Sept 2003)). With a firewall protecting the network from unauthorised ingress traffic and unauthorised egress traffic, the perimeter will have an acceptable level of defence. Use of automatic update services provided by operating system manufacturers will also provide an acceptable first line of defence against new client vulnerabilities.

Note that best practice would involve separating services across individual machines, as a remote exploit affecting the firewall, DNS or mail services would instantly provide access to the internal network – however due to the cost and other considerations outlined above, a medium has to be found between the acceptance of the risk and the cost of increased security. Performing regular maintenance and updates will help mitigate some of this risk.

5. Configuration and hardware requirements

Requirements for a functional home network are similar to a small corporate network, although financial restrictions would prevent the same level of availability and recovery. It is assumed that the home has RJ45 wall outlets throughout the rooms connected to a patch panel in a central location (such

as a loft, under stairs cupboard etc.) where a switch and a server or servers can also be located. Ventilation and fire prevention should be taken into account, as the equipment will be left powered on constantly and accumulation of heat or component failure will present a fire hazard. Sufficient power capacity must also be present to prevent cable overheating and / or damaging of fuse or circuit breakers – in the UK, two correctly wired dual outlets should be sufficient.

Based on the device requirements mentioned above, 8 devices would initially be in use, possibly requiring 10 switch ports. A standard 24 port switch should provide enough capacity for future proofing at a minimal cost, provided configuration changes require some measure of authentication. Taking into consideration the purchase and power costs of running multiple devices, the main network services will be provided by a single server acting as a single point of entry/exit to the home network, and also providing internal services such as file storage. Ideally this should be split into several machines providing separate firewall, DNS, web server and email traffic, and an internal server – however as outlined above this is not a feasible approach for a low budget home network. Security and availability must be balanced against cost and available space.

The network connection will be provided via an ADSL service – for the purposes of this paper, this is based on a package provided by a UK ADSL provider, and presented to the network via an ADSL router in bridge mode directly connected to the firewall. This package provides a 1Mb/s down, 256k up connection with 8 consecutive public IP addresses. This means basic configuration is stored on the router device, with authentication information being stored on the firewall itself – mitigating the risk of the embedded router device exposing information should a vulnerability exist. The usual bridge method used for these devices is to use a PPP tunnel between the firewall and the router device, with authentication information being supplied by the firewall directly through to the service provider.

Processing power requirements are minimal for OpenBSD's pf – (Nick Holland, PF : Performance, http://www.openbsd.org/faq/pf/perf.html Rev. 22 Sept 2003), particularly in this application. The firewall ruleset will be small, and traffic will not rise above 1Mb/s through the firewall. This means an older machine can be re-used, although it must have sufficient capacity for file sharing internally. This machine will also require 3 network cards – one for the interface to the router, one to connect to the internal network, with the third providing the optional DMZ as outlined above.

Due to the nature of the OpenBSD operating system, minimal configuration is required to provide a high level of security, and configuration can easily be backed up for restoration should the system fail – this can be done by archiving configuration files nightly and copying them to CD or tape drive.

User data stored on the server may also require backup – this will depend on the type of data stored, and whether a decision is made to only store data on the central server or on local machines. If data is stored on the server and will

need to be recovered, a tape drive is recommended due to cost and capacity – a legacy DAT drive should be sufficient.

The main server can also provide an external DNS service, public facing web server (for external mail access) and external SSH access (for remote administration) as well as providing a mail server to receive mail. It is recommended if possible that DNS, web and email services are provided by a third party or hosted on a separate machine within the network due to security risks. Increasing the number of publicly available services from one machine increases the risk of compromise (the entire machine could be compromised through one service).

Client machine specification will be dictated by user and financial requirements, although it is expected that user desktops will be current models – these will run either Microsoft Windows XP or Redhat 9. The web desktop machine will run Redhat 9 with a minimal configuration, so can be a lightweight client such as a mini-ITX machine.

Further redundancy can be added as space, power and finance allows, allowing redundant desktop machines to be used as additional servers to split services away from the firewall. In this situation, port forwarding on the firewall can be used to provide those services.

6. Configuration process

Configuration will be based on a simple private internal network with NAT being performed on the firewall. The IP addressing provided by the ADSL provider allows for 5 usable IP address out of the 8, as 3 are used by the network, broadcast and router addresses. The remaining 5 addresses will provide a public IP address for the firewall, DNS and web services (if present), a public IP address which will only be used to NAT egress traffic with (hide address), and 3 spare public addresses for future use. The internal network will use a class C network within the 192.168.0.0-192.168.255.255 private address range as defined in RFC 1918 (RFC1918, http://www.rfc-editor.org/rfc/rfc1918.txt, Feb 1996), with a range of addresses provided by DHCP to the internal network.

6.1. Network device configuration

The ADSL router should be configured to act as a bridge device between the ADSL line and the Ethernet network (manufacturers can refer to this as either half-bridge mode or bridge mode – depending on implementation either can be correct). This presents a PPP tunnel endpoint which is connected to by the firewall. If possible a backup of the configuration should be made.

The switch should be configured with a complex password to prevent unauthorised changes, and ideally each port should be restricted to the MAC address of the connected device, providing an additional layer of security against devices being connected to the network. A backup of the

configuration should be taken as well as ensuring the configuration is saved in case of power interruption.

6.2. Firewall configuration

Note this is based on OpenBSD release 3.3. References to package names are relevant to this release only, although future releases use incremental numbering systems.

Installation should be performed according to recommendations for installation of an OpenBSD base system (OpenBSD FAQ 4, http://www.openbsd.org/faq/faq4.html, August 2003). Required packages for the install are : bsd, base33, etc33, comp33 and man33. It is recommended that a full CD set be purchased to provide source code.

Once this is installed, update the server with any required patches, following guidelines within http://www.openbsd.org/errata.html (OpenBSD Errata, http://www.openbsd.org/errata.html, Date unknown).

The following should also be configured on the firewall;

Pf : configure pf to a basic ruleset blocking all traffic in except 22/tcp - ssh (for remote management) and 53/tcp+udp (for DNS lookups) and 80/tcp outbound (for external web access). Post install, additional rules can be configured to provide access to required services, both inbound and outbound. The firewall logging device, pflog0, should also be brought up and the pf logging daemon (pflogd) should be running. This will allow analysis of dropped traffic.

Unused services : while OpenBSD ships with unnecessary services disabled by default, checks should be made to ensure that nothing is running that is not explicitly required. The “man afterboot” command within OpenBSD details additional similar steps.

sudo : never login directly as the root user, either from the console or remotely. Instead configure the “wheel” group and the “/etc/sudoers” file to provide nominated users with required additional privileges.

ssh : configure the ssh server (sshd) as required. For home use, as a minimum decrease concurrent connections, apply a timeout and add a warning banner for pre- and post-logon. The logging level should also be increased to provide more detailed information about successful and failed authentication attempts.

Mail aliases : modify the “/etc/mail/aliases” file to redirect mail as appropriate – either to another user on the server or to an external address. Security audit information (this runs as a script from cron) can then be reviewed when sent.

6.3 Internal server / firewall additional configuration

The following applications and services should be installed according to their installation guidelines ;

- Djbdns (D. J. Bernstein, http://cr.yp.to/djbdns/install.html, Date unknown). Note this is only required if mail and DNS services are needed. Further discussion of DNS setup is outside the scope of this document. This choice of DNS implementation is made based on observed security and lack of vulnerabilities.
- Squid – install and configure with pf (Daniel Hartmeier, Transparent Squid, http://www.benzedrine.cx/transquid.html, Date unknown (rev. 22 Sept 2003))

Optional services;

Email spam protection : due to the high proportion of spam mails, it is worthwhile installing and configuring a spam filter; SpamAssassin (SpamAssassin, http://www.spamassassin.org, Date unknown) is a highly suitable application for this and can be installed either on a machine acting as your mail gateway (How to install SpamAssassin on OpenBSD with Sendmail, http://davespicks.com/writing/programming/spamassassinopenbsd.html, 12/03/2003) or on the individual client machines.

Intrusion detection : residential subnets such as those provided for home ADSL / cable clients are usually subject to a high level of scans and compromised machines originating attacks or scans; due to many home machines not being kept secure and up to date, these machines make easy targets (or 'low hanging fruit') to use as platforms for further attacks, such as distributed denial of service.

An intrusion detection system (whether host or network based) present on this home network would need to be configured carefully to prevent alert fatigue (e.g. from repeated false alarms caused by harmless scanning) and to ensure that warning messages are generated on directed attacks. It is expected that most attacks directed towards the home network will be from 'script kiddies' or previously compromised / infected machines and not concentrated direct attacks (it is unlikely highly sensitive or classified information will be present on the home network) from experienced system crackers.

Snort (Snort, http://www.snort.org, date unknown) provides a free and fully functional signature based intrusion detection system. This can be run on the firewall itself or placed internally or externally, depending on what the home user deems a higher threat (attacks within the secured environment or external to it). Signatures are provided and updated regularly by the community, and rules and alerts can be tailored to provide an acceptable level of alerting. Guidelines for the use of Snort within an OpenBSD environment can be found at http://www.teamrci.net/acid_openbsd.html (Rex Consulting, Installing ACID, Barnyard, and Snort on OpenBSD 3.3, http://www.teamrci.net/acid_openbsd.html, 2003)

7. Post install information gathering and configuration

Following installation as above, the firewall will block all traffic except inbound 22/tcp (potentially also inbound 80/tcp, 53/tcp+udp and 25/tcp depending on configuration – see above) and all outbound traffic apart from 53/tcp+udp, 80/tcp and 22/tcp. This restrictive set of rules allows for basic domain lookups and web browsing from within the network, and remote management via SSH from the internet. Given the requirement for this network to provide services for a family, additional rules are likely to be needed to allow other services such as IRC, instant messaging as well as SSL web traffic.

With the clients connected to the network, an attempt at usual network activity should now be made – such as connecting to 'feature-rich' web services, messaging / chat and other commonly required activities. Most of these that rely on services other than DNS and web traffic will fail, but the pflogd daemon will log the dropped ingress and egress traffic. Using a tool such as Ethereal (Ethereal site, Introduction to Ethereal, http://www.ethereal.com/introduction.html#features , 14/11/2003) (using a GUI, or command-line tools such as tcpdump (tcpdump team, tcpdump site, http://www.tcpdump.org/, 13/11/2003) will show what traffic is being dropped which then allows the firewall ruleset to be updated as below.

It should be noted that 'opening' the firewall to allow the required services through should not be based solely on one test run. Services such as Microsoft's Instant Messenger (Microsoft, MSN Messenger site, http://messenger.msn.com/ , Date unknown) attempt connections to multiple addresses before failing, and components within some web pages (such as ActiveX controls) will attempt connections to resources that may not be desirable. These dropped packets should be examined along with the activity attempted; for example, a connection to a web site that uses embedded Java or ActiveX components may obtain content from within a local applet – this could be advertising, behaviour monitoring or some other undesired activity. While the web site and other components may be fine, these kinds of activity should be noted as an individual connection (generally, a web page will function as intended without these components) rather than taking the series of connection attempts following a web page request as requirements for a successful page load. A high level example of this is as follows;

Outgoing - DNS lookup for www.somewebsite.tld
Incoming – Response of 1.2.3.4
Outgoing – HTTP GET request for web site
Incoming – HTTP page load
Outgoing – Image downloads from page content
Outgoing – HTTP POST request to 2.3.4.5
Outgoing – HTTP GET request to 3.4.5.6

This shows a page request being made by a device. The initial DNS lookup and HTTP traffic to the web server are what would be expected, however there are subsequent HTTP GET and POST requests to a different location. In this instance, these may simply be a hit counter for the website. While

browser settings help mitigate this kind of threat, careful monitoring at this discovery stage is important to prevent an 'allow everything' philosophy.

Following this stage, normal or expected use should be possible. Once this is achieved by repeating the above process until satisfactory (note that this will be an ongoing process through the life of the network). At this stage, bandwidth usage can start to be limited; using pf with altq for traffic queuing (OpenBSD team, PF: Queuing, http://www.openbsd.org/faq/pf/queueing.html, 9/11/2003) will allow allocation of bandwidth to required applications. Provided the border router device on the network is capable of SNMP, MRTG (MRTG, http://people.ee.ethz.ch/~oetiker/webtools/mrtg/, Date unknown) can be used to graph traffic statistics;

- Install and configure MRTG to monitor the router
- Collate statistics based on observed behaviour over a reasonable period of time
- Implement queues based on this information using altq and pf.

As a rough guide, the following proportions are likely to result from this behaviour (please note that these are taken from observed behaviour on a similar network and are an approximate guide only);

- Corporate laptop 9%
- DNS traffic 1%
- Web browsing 10%
- Data transfers 80%

Note that data download speeds from the internet to the home network are affected by the rate of the uplink speed – with the ADSL connection used for this document, the given rate is 1Mb/s downlink and 256k/s uplink. If an ideal download speed is achieved, this can be limited by the speed of return packets (this observation is based on Daniel Hartmeiers empty ACK prioritisation page (Daniel Hartmeier, Prioritizing ACKs, http://www.benzedrine.cx/ackpri.html, 25/9/2003))

Prioritising empty ACK packets (rather than simple outgoing requests) can help increase overall throughput due to this, as shown on the referenced page.

The next step is restricting bandwidth either by host(s) or by service. This will allow all services within the network to operate within reasonable parameters – for example, multiple data transfers such as downloads can be limited to a percentage of bandwidth so that other users will not be affected. This will reduce download speeds, but will allow all users to experience consistent performance.

8.Testing

Following the information gathering phase and firewall configuration, each device will need to be tested for functionality. This should include normal web browsing, email, online gaming – both from personal computers and any games consoles – and any other usual activity such as instant messaging. FTP should also be tested, as firewall configuration may prevent successful connections for passive FTP.

Additionally, remote access to the network should be tested from an external network, to ensure that remote connectivity is possible. This should cover SSH access and any other services that have been made available such as a public facing web server, DNS server or SMTP server.

Following this testing, it is advisable to perform a penetration test against the home network from a remote location. This should cover the following steps;

- Full port scan over the entire subnet (or single IP). Tests should cover basic connect scans as well as more complex options such as null and half scans. If possible use tools such as nmap (Fyodor, nmap intro, http://www.insecure.org/nmap/index.html, date unknown)
- Vulnerability scan over entire subnet (or single IP). This should be performed with tools such as Nessus (Renaud Deraison, Nessus introduction, http://www.nessus.org/intro.html, date unknown)
- Use of network mapping tools to attempt to discover address ranges, and machines behind firewalls. Tools such as FireWalk (Mike D. Schiffman and David Goldsmith, FireWalk, http://www.packetfactory.net/firewalk/, 27/1/2003) use traceroute techniques to attempt to map devices behind a firewall.

Scans should also be performed from within the home network against agreed hosts to test for outbound firewall rules.

Results from these tests will highlight any security concerns around firewall rules, services and connectivity. Corrective action can then be taken to prevent these issues. If this is required, the penetration test should be performed again to ensure that changes have not caused any additional security issues.

9.Tuning

Once the firewall and bandwidth control have been configured, normal use over a short period of time will show if there are any speed or other issues concerning the bandwidth limitations. This also applies to the transparent HTTP proxy service (if used) – guidelines for tuning the cache for the proxy can be found at http://squid.visolve.com/squid24s1/cache_size.htm (Squid / Visolve, Cache configuration, http://squid.visolve.com/squid24s1/cache_size.htm, 15/5/2002). Cache

refresh and aging settings should be configured as appropriate for observed usage through a test phase.

10.Maintenance guidelines

Maintenance of the home networking environment is essential. One of the primary items for maintenance is ensuring that operating systems and applications within the home environment are kept up to date with security patches and service packs. For Microsoft Windows clients, Automatic Updates can be configured to automatically download and install patches and updates without prompting, although it is recommended that any updates are researched before applying to ensure that no issues arise from the installation. For other operating systems within the network, including the OpenBSD server(s), it is recommended to subscribe to security lists such as BugTraq as well as any vendor-provided notification service.

If an intrusion detection system has been configured to provide alerts, it is essential to ensure that the IDS is kept up to date with current signatures. Any anti virus products and anti spam products must also be kept current to provide accurate and timely detection and prevention of virii and unsolicited email.

Additionally, OpenBSD provides a regular security information mail detailing changes and concerns that may occur such as file system changes, SUID files and other changes. Alerts such as these, those from the IDS system and any security alerts should be monitored regularly.

It is highly recommended to perform regular penetration tests against the home network to ensure that no services or devices have been neglected and that no unexpected services or devices are attached to the network. These regular tests should also be carried out from within the network against the internal machines.

11. References

CERT, “Home Network Security”, URL : http://www.cert.org/tech_tips/home_networks.html (December 2001)

Alex Sands, Security Focus, URL : http://www.securityfocus.com/news/490, (June 19 2002)

Brian R. Krause, Usability : A Requirement for Security, URL : http://www.encentuate.com/perspectives/usability.htm (Date unknown)

Alma Whitten and J. D. Tygar, Usability of Security : A case study, URL : http://secinf.net/cryptography/Usability_of_Security_A_Case_Study.html , (December 18, 1998)

Daniel Hartmeier, Transparent Squid, URL : http://www.benzedrine.cx/transquid.html, (Date unknown, revision from Monday 22 Sept, 2003 used)

Nick Holland, PF : Performance, URL : http://www.openbsd.org/faq/pf/perf.html (Date unknown, revision from 22 Sept 2003 used)

RFC1918, URL : http://www.rfc-editor.org/rfc/rfc1918.txt, (Feb 1996)

OpenBSD FAQ Team, OpenBSD FAQ 4, URL : http://www.openbsd.org/faq/faq4.html, (August 2003)

OpenBSD Errata, URL : http://www.openbsd.org/errata.html, (Date unknown, revision used 17 Sep 2003)

D. J. Bernstein, URL : http://cr.yp.to/djbdns/install.html, (Date unknown)

SpamAssassin team, SpamAssassin, http://www.spamassassin.org, (Date unknown)

Dave Polasheck, How to install SpamAssassin on OpenBSD with Sendmail, URL : http://davespicks.com/writing/programming/spamassassinopenbsd.html, (12 Mar 2003)

Snort team, Snort home page, URL : http://www.snort.org, (Date unknown)

Rex Consulting, Installing ACID, Barnyard, and Snort on OpenBSD 3.3, URL : http://www.teamrci.net/acid_openbsd.html, (2003)

Ethereal team, Ethereal site, Introduction to Ethereal, URL : http://www.ethereal.com/introduction.html#features , (14/11/2003)

tcpdump team, tcpdump site, URL : http://www.tcpdump.org/, (13/11/2003)

Microsoft, MSN Messenger site, URL : http://messenger.msn.com/, (Date unknown)

OpenBSD team, PF: Queuing, URL : http://www.openbsd.org/faq/pf/queueing.html, (9/11/2003)

MRTG team, MRTG, URL : http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ , (Date unknown)

Daniel Hartmeier, Prioritizing ACKs, URL : http://www.benzedrine.cx/ackpri.html, (25/9/2003)

Fyodor, nmap introduction, URL : http://www.insecure.org/nmap/index.html, (date unknown)

Renaud Deraison, Nessus introduction, URL : http://www.nessus.org/intro.html, (date unknown)

Mike D. Schiffman and David Goldsmith, FireWalk, URL : http://www.packetfactory.net/firewalk/, (27/1/2003)

Squid / Visolve, Cache configuration, URL : http://squid.visolve.com/squid24s1/cache_size.htm, (15/5/2002)