

Academic Scientific Research Network of Armenia (ASNET-AM) Network Security Technical Report 2006-2007

Arthur Petrosyan

arthur@sci.am

Academic Scientific Research Network of Armenia (ASNET-AM)

Institute for Informatics and Automation Problems (IIAP)

of the National Academy of Sciences of Armenia (NAS RA)

<http://www.asnet.am>, <http://www.sci.am>

December 1, 2007

Table of Contents

1. Introduction	3
2. Use of Free and Open Source Software in ASNET-AM	3
3. Layered Security Approach	4
4. Perimeter Security	5
5. IDS / IPS	6
6. Network Connection Encryption	6
7. VPN	7
8. E-mail Security / Anti-SPAM	7
9. Virus Protection	8
10. TCP Wrappers	10
11. Web Server / Database Security	10
12. Password Security	11
13. Logfiles	12
14. Backup	12
15. Security Incidents Handled	13
16. Conclusion	13

1. Introduction

Academic Scientific Research Network of Armenia (ASNET-AM, <http://www.asnet.am>) is a largest REN in Armenia which unifies Academic, Scientific, Research, Educational, Cultural and other organizations, which are engaged in scientific and educational activity. ASNET-AM unites scientists, scientific and technical associates, post-graduates, students and other users from more than 50 scientific, research, educational, cultural and other organisations.

ASNET-AM is joint structure of 4 laboratories of Institute for Informatics and Automation Problems (IIAP) of the National Academy of Sciences of the Republic of Armenia (NAS RA): Laboratory of Mathematical Support for Distributed Systems (LMSDS), Laboratory of Network Administration (LNA), Laboratory of Network Communications (LNC) and Laboratory of High-Performance Computing Systems (LHPCC).

ASNET-AM was created in 1994 and since then we are striving for establishing a secure and stable network structure. Furthermore, ASNET-AM in cooperation with recently established CERT AM/AM NREN CSIRT (<http://www.cert.am>) continues implementing various security technologies and managing prevention, investigation and liquidation of computer incidents.

In an effort to provide secure and reliable network environment the technical staff of ASNET-AM has been implementing several security procedures during 2006-2007, which are described below. These procedures can be viewed as best practices that introduce the more critical aspects of securing a network.

2. Use of Free and Open Source Software in ASNET-AM

Use of free and open-source software (FOSS) in ASNET-AM gives us the right to run, copy, distribute, study, change, and improve it as they see fit, without having to ask permission from or make fiscal payments to any external group or person. The autonomy properties of FOSS make it useful for ASNET-AM applications such as rapid responses to cyber-attacks, for which slow, low-security external update processes are neither practical nor advisable, and for applications where rapid, open, and community-wide sharing of software components is desirable.

FOSS is vital to ASNET-AM Information Security and FOSS applications and strategies play major role in the security implementations at ASNET-AM. Not using FOSS in this area would have immediate, broad, and in some cases strongly negative impacts on our ability to protect ASNET-AM against hostile intrusion. This is in part because it would prevent us from using the same analysis and network intrusion applications that hostile groups could use to stage cyber-attacks. It would also remove the uniquely FOSS ability to change infrastructure source code rapidly in response to new modes of cyber-attack.

The FOSS communities contribute to ASNET-AM security in several ways. First, they produced infrastructure software such as [Slackware Linux](#) with low rates of software failure

combined with early and rapid closure of security holes, which makes such systems useful as the security linchpins in broader security strategies. Also, the FOSS communities have had a long-term fascination with developing more and more sophisticated applications for identifying and analyzing security holes in networks and computers, resulting in FOSS products such as [Snort](#), that are invaluable to in-depth analyses of security risks.

As it can be seen there is a plethora of reliable FOSS (OS, packages, utilities) for establishing, maintaining and monitoring secure systems and networks. And cost isn't the only reason for using FOSS. Most of Research and Educational Networks (RENs) often tend to use FOSS for a number of other reasons (many Scientific and Research packages are FOSS). Besides, FOSS and proprietary software can work well together.

Following is the alphabetical list of FOSS applications used in the ASNET-AM during 2006-2007 for security implementation:

CenOS Linux, Chkrootkit, COPS, Crack, DenyHosts, Expect, Ettercap NG, FreeRadius, Ganglia, Globus Toolkit, IPTraf, Lsof, MRTG, MySQL, MySQL-cluster, Nagios, NETAMS, Netwatch, Network Weathermap, Nmap, Ntop, OpenSSH, OpenSSL, PHP, Red Hat Linux, Rkhunter, RRDtool, Rssh, Scientific Linux, Slackware Linux, Snort, Spamassasin, Sqstat, Squid, Stunnel, TCP Wrappers, Tripwire, Vtun.

3. Layered Security Approach

The layered-security approach in ASNET-AM centers on maintaining appropriate security measures and procedures at five different layers within network environment:

1. **Perimeter Layer**
2. **Network Layer**
3. **Host Layer**
4. **Application Layer**
5. **Data Layer**

The table below presents the layered-security model used in ASNET-AM and some of the technologies that function at each level.

	Security Layer	Applicable Security Measures
1.	Perimeter Layer	<ul style="list-style-type: none"> • Network Firewall • Network-based Anti-virus/AntiSPAM • VPN encryption
2.	Network Layer	<ul style="list-style-type: none"> • Intrusion detection/prevention system (IDS/IPS) • Network access control • Access control/user authentication

3.	Host Layer	<ul style="list-style-type: none"> • Host Firewall/IDS • Network access control • Host Anti-virus/AntiSPAM • Access control/user authentication
4.	Application Layer	<ul style="list-style-type: none"> • Application shield • Access control/user authentication • Input validation
5.	Data Layer	<ul style="list-style-type: none"> • Encryption • Access control/user authentication

Before presenting a more detailed discussion of implementations of security measures mentioned above in, it should be mentioned about the effect of layered approach for securing the network.

Network security professionals speak in terms of “work factor”, which is an important concept when implementing layered security. Work factor is defined as the *effort required by an intruder to compromise one or more security measures*, which in turn allows the network to be successfully breached. A network with a high work factor is difficult to break into, while a network with a low work factor can be compromised relatively easily. If hackers determine that our network has a high work factor, which is a benefit of the layered approach, they are likely to move on and seek some other networks that are less secure — and that’s exactly what we want them to do.

Due to the efforts done in the field of network security during years of 2006-2007 ASNET-AM can be identified as a network with a high work factor. Details presented in this report prove this statement to be true.

4. Perimeter Security

Firewall protection is the first line of network security in ASNET-AM. Both hardware-based firewalls (Cisco routers and other) and Linux/UNIX-based firewalls are effectively used to provide control/filtering over the flow of information between ASNET-AM and outside world. All currently unused ports/addresses are being strictly filtered.

Filters installed on ASNET-AM firewalls can control traffic between external hosts and all internal hosts. Services and hosts that do not need to be visible from the external network are blocked at the firewall immediately reducing the risk of external attack against those machines. The effort required to enforce good security on individual hosts can then be concentrated only on the small subset of hosts and services which are visible from the outside.

Such approach helps to limit the (lower) layers job to control only used/opened services/ports/addresses. Although some redundancy exist in current layered implementation, this has been done intentionally in order to extend security. Such redundancy means that

some restrictions on the upper layer(s) are duplicated on lower layer(s), which is like having more than one locked door to open until you reach the destination room.

5. IDS / IPS

A valuable part of network security layer is Intrusion Detection/Prevention System (IDS/IPS), which is functioning as a “Burglar alarm system” for the network. Snort package is currently considered de facto standard for intrusion detection/prevention.

Other additional packages are also used ([Sentry tools](#), [DenyHosts](#), etc.) to detect and block various attacks. For example, about 600 brute force attacks per month were detected and blocked in ASNET-AM during 2006-2007.

6. Network Connection Encryption

In some cases it is important to be concerned about disclosing information that is transferred through the network. Certainly it is not desirable that someone could access an account that is not theirs or capture personal information that may be transmitted over a network. When one wishes to avoid data disclosure over a network, encryption methods must be employed that make the transmitted data unreadable to someone who might somehow capture the data as it traverses a network. There are many methods to “encrypt” data and all major methods described below are being effectively used in ASNET-AM.

Network communications programs like telnet, ftp, and the "r commands" (rlogin, rcp, rsh and rexec) may transmit the username and password across the network in the clear making it easy for a sniffer to capture this information. Various networking solutions are installed in ASNET-AM to provide the necessary connectivity for users while encrypting all session-traffic (including the password) to reduce the threat of password sniffing and TCP session hijacking.

Major solutions include use of:

- SSH instead of Telnet
- SFTP instead of FTP
- [STUNNEL](#) (Universal SSL Wrapper) for encapsulation of POP3 and IMAP
- Secure Socket Layer (SSL/HTTPS) for HTTP

The solutions listed above are mostly oriented on the use of SSH ([OpenSSH](#)) and SSL ([OpenSSL](#)) protocols that employ various cryptographic mechanisms to provide security through authentication and encryption methods. Services like telnet and ftp are mostly disabled on ASNET-AM servers and secure protocols are used instead.

It should be mentioned though, that the level of security provided with all the above is dependent upon many things such as the cryptographic methods used, the access to the transmitted data, algorithm key lengths, server and client implementations and most importantly, the human factor. The most ingenious crypto scheme is thwarted if a user's

access credential, such as a password or certificate, is obtained by a third party. The classic case is the user's password on a Post-It note on his/her monitor.

7. VPN

Manu VPN realizations currently exist (PPTP, IPIP, GRE, PPP atop SSH, IPsec, FreeS/WAN, CIPE, etc.) and some of them are used in ASNET-AM. Additionally another effective VPN tool called [VTUN](#) was introduced in ASNET-AM during 2006-2007.

VTUN is very simple client-server VPN tunnelling application with wide spectrum of options like different levels of tunneling (IP, PPP/SLIP, Ethernet), encryption (BlowFish 128 bits), compression (zlib, lzo), traffic shaping, etc. VTUN can work both over TCP and UDP and uses universal TUN/TAP device driver, which is already included in the kernel of many UNIX distributions. VTUN is many-to-one application and it has proved to be very effective FOSS solution for VPN. A number of secure virtual tunnels were installed and are operating in ASNET-AM with the use of VTUN package.

An application of VTUN package together with Policy Routing methods is effectively used in ASNET-AM as a solution of routing problems in distributed networks, where basic problem of routing is the obligation for each router to have only one default route. It means, that in the presence of several links to the external networks, for each such link separate router will be necessary. By using Linux kernel features of advanced routing and with the help of VTUN package for VPN creation and IPRROUTE2 package for policy routing more effective solution is being provided.

8. E-mail Security / Anti-SPAM

In an effort to blocking unsolicited junk E-mail messages (SPAM) three primary methods are used:

1. RBLs (Realtime Block List)
2. Static Block List
3. [Spamassassin](#) package

During 2006 and till the June of 2007 the following 11 RBLs proved to be effective at ASNET-AM:

- spamcop.net
- spamhaus.org (sbl, xbl)
- dsbl.org
- abuseat.org
- spambag.org
- dul.ru
- ahbl.org
- njabl.org
- ordb.org
- msrbl.net
- dul.dnsbl.sorbs.net

The analysis of RBLs effectiveness done in June, 2007 (presented in the table below), showed that 3 of them are useless.

	<i>RBL</i>	<i>Monthly Number of Spam Attempts Rejected</i>
1.	spamcop.net	207912
2.	spamhaus.org	115767
3.	dul.dnsbl.sorbs.net	77155
4.	dsbl.org	9762
5.	dul.ru	3562
6.	cbl.abuseat.org	1269
7.	ahbl.org	449
8.	spambag.org	232
9.	msrbl.com	13
10.	ordb.org	30
11.	njabl.org	0
	TOTAL	416151

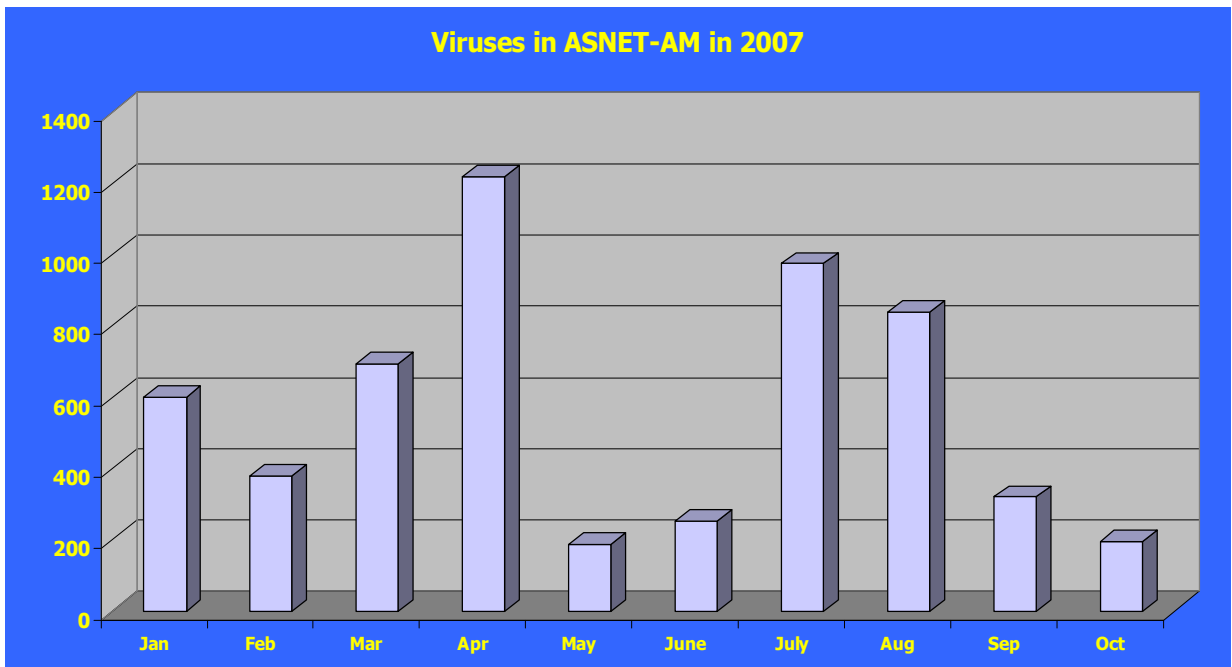
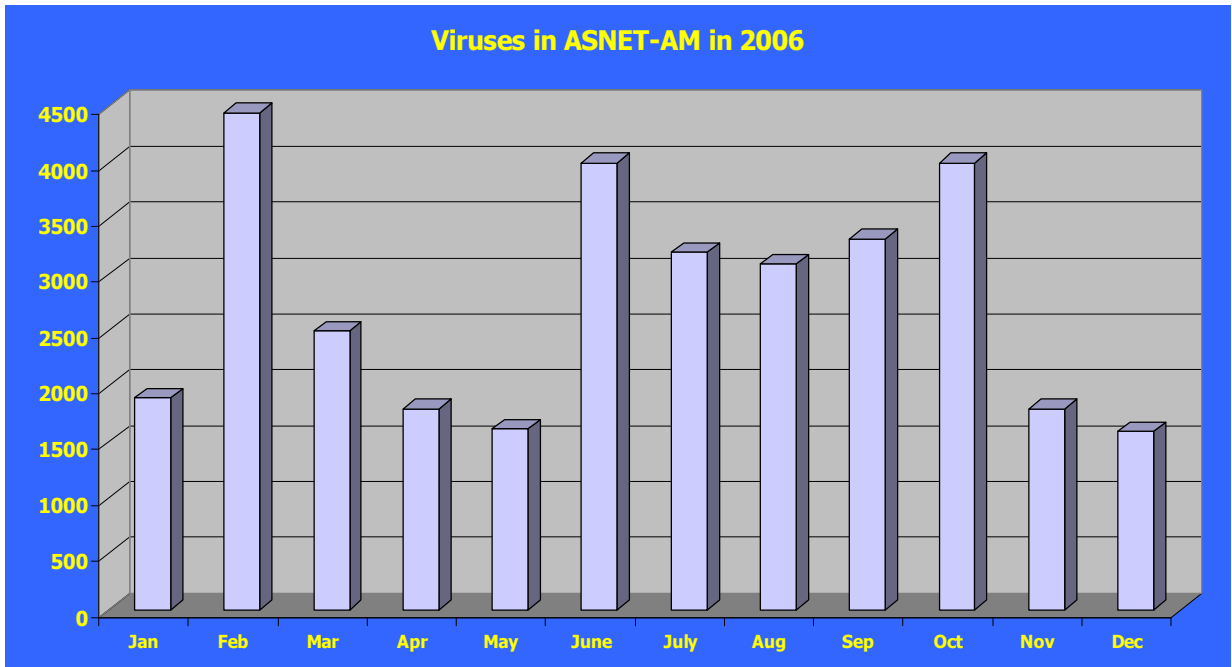
Decision to remove 'njabl.org', 'ordb.org' and 'msrbl.com' RBLs was made and remaining 8 RBLs are currently functioning very effectively. The average attempts blocked using the above 8 RBLs during last months has reached the number of **921000/monthly**.

Static Block List is just a small addition to the existing RBL mechanism, which has no big impact on the percentage of Spam blocked, but rather gives opportunity to block instantly anything required (Source E-mail address/IP address). This is very useful in case of E-mail flooding from somewhere.

Spamassassin package was installed in ASNET-AM only in 2007, so the use of it is still on the very initial stage with the standard configuration and "required_hits" set as high as 8.0. More fine tuning is still in progress with Spamassassin, to assure its more effective usage. Current effect from the use of Spamassassin in ASNET-AM is the following: average attempts blocked – **12000/monthly**.

9. Virus Protection

There is no question that every network needs to be protected from viruses. ASNET-AM has implemented a centralized E-mail virus protection system. The results of E-mail virus protection system work in 2006-2007 are presented in the figures below.



10. TCP Wrappers

TCP wrappers allow the administrator to log connections to TCP services - primarily those launched by the inet daemon. It also can restrict incoming connections to these services from systems via two files, hosts.allow and hosts.deny. Both of these features can be very useful when tracking or controlling unwanted network connection attempts.

TCP Wrappers can be viewed as a security layer to monitor and control UNIX server's incoming TCP traffic on application level. It is very flexible way to configure per address access control for those applications/ports that are needed to be open (using /etc/hosts.allow, /etc/hosts.deny files).

TCP Wrappers mechanism in ASNET-AM is mostly used for services like SSH/SFTP on a servers, where access can be strictly limited per IP address. Additionally, since TCP Wrapper support (also called "libwrap support") is mostly compiled into the sshd binary, it is widely used in ASNET-AM by DenyHosts package to block SSH brute force attacks.

11. Web Server / Database Security

Although the use of SSL helps in securing web traffic, it is still required to ensure the security of Web server itself. Much attention is paid in ASNET-AM to the security configuration of Web servers to prevent Web server attacks. Web server attacks encompass a wide variety of problems with nearly every Web server available. From simple page defacement, to remote system compromise, to a complete denial of service (DOS), Web server attacks are one of the most common attacks today.

Most of Web servers in ASNET-AM are UNIX/Linux based [Apache](#) Web servers which is considered to be most reliable and widespread Web server FOSS package. Of course, nothing is secure in default configuration and any system/application requires proper configuration. The same is true with Web server configuration and following security steps, which are effectively implemented in ASNET-AM, can provide extended security for Apache Web server:

- Hiding Apache version ('ServerTokens Prod', 'ServerSignature Off' in httpd.conf)
- Disable TRACE and TRACK methods
- Critical data not stored on the Web server itself if possible (reverse proxy or remote database)
- Storage of static content on a read-only media (CD-ROM) in specific cases
- Running Web server on non-standard port where applicable
- Controlling access to Web server's IP/port on Firewall level
- On dual-homed hosts bind Web server only to the required IP address/network interface

- Not trivial directory name for Website CMS (backend) part (<http://mywebsite.domain.com/admin> is a bad choice)
- Securing directories by Apache AAA mechanism (.htaccess) where applicable
- Not using FTP or telnet for data transfer to/from Web server (using SSH or SSL instead)
- Chrooting Web server and each Web hosting user

Many Web servers are currently integrated with the database servers. Classic example is Linux-Apache-MySQL-PHP (LAMP). So, security of the database servers is also a separate issue. ASNET-AM database servers are secured in several ways:

1. running database server on non-standard port
2. binding database server to local to localhost (127.0.0.1) only where applicable (if database server is located on the same host as the Web server) or only to the required IP address/network interface
3. controlling access to database server's IP/port on Firewall level

12. Password Security

Humans are truly the weakest link in any security field. Most people are not careful about keeping secrets such as passwords that form the basis for most secure systems. All security systems rely on a set of measures employed to control access, verify identity and protect disclosure of sensitive information. These measures usually involve one or more "secrets". Should a secret be revealed or stolen then the systems that are protected by these secrets can be compromised.

It may seem like a terribly obvious statement, but most systems are compromised in very basic ways. Leaving a Post-It note with a system password stuck to the side of a computer monitor may seem foolish, but many people in fact do such things. Another example, which is only slightly less obvious, is the tendency to set very trivial passwords, like setting password the same as the username.

Basic rules that are required to be followed for usernames and passwords within ASNET-AM servers include:

- Not using obvious passwords such as own name, telephone number, date of birth, etc.
- Use longer passwords with mixed numbers or symbols (at least 8-10 characters or more)
- Change passwords on a regular basis or at least mix them by changing/adding some characters there

- NEVER leave credentials in publicly accessible place (such as Post-It note on a computer monitor)

Of most importance is server administrator's password – root password. Several important measures are taken in ASNET-AM to protect root password. No user is generally logging in directly as 'root', while connecting over the network ('PermitRootLogin' option in /etc/ssh/sshd_config file is set to 'no' for SSH). Root login is permitted only from the server's console. Administrators are logging in with their own accounts, and then use 'sudo' package to gain limited root privileges.

The 'sudo' utility allows to set limited privileges for specified user accounts. Strict actions (files/commands) that can be taken by these accounts can be specified in '/etc/sudoers' file. No need to know root password, specified user can gain limited privileges by entering his own password.

Additional security measure taken in ASNET-AM servers is setting timeout for logged in users, so they have to re-authenticate after short period of time in order to use 'sudo' (setting 'TMOUT' Shell Variable in /etc/profile).

All the above measures ensure accountability of privileged users and increase the security level.

13. Logfiles

Logfiles are one of the most useful tools in detecting and investigating any problems with computer systems and particularly network security issues. Logs can provide information about system faults and misuse as well as early warnings of problems. Without collecting and analysing logfiles, it is impossible to know what is happening on the network.

Many security procedures and tools described above rely on the information provided from various log files.

14. Backup

Data backup is necessary to protect users from losing data whenever the system is compromised or when there is a hardware issue (e.g. disc breakdown).

Regular backup of valuable data is scheduled in ASNET-AM. Multifunction backup package is currently used. This package was developed in ASNET-AM and it allows to implement network based backup with duplication of backed up data both locally and remotely. Some of the features of the package are:

- Backup files compression with GZIP/BZIP2
- Secure network transmission with SCP/SFTP
- E-mail notification upon successful backup completion

Future replacement of currently used backup package with Bacula program is being considered. Bacula network based backup program is actively developed and full-feature backup FOSS solution with administration Web interface.

15. Security Incidents Handled

Due to the efforts described above ASNET-AM has a high work factor. This means that much effort is required by an intruder to compromise our network, which is a benefit of the layered approach used. Thanks to that the ASNET-AM has experienced only 3 succeeded security incidents during 2006-2007, which were instantly handled.

1. Simple defacement of experimental testing Web page hosted at ASNET-AM. Initiated on September 13, 2007 23:19 (GMT+4). Fixed instantly.
2. Compromise of Web page hosted at ASNET-AM using errors in PHP script, with UDP Flooding initiation followed. Initiated on July 20, 2007 08:29 (GMT+4). Caused termination of network connection within that network segment for about 3 hours.
3. Succeeded brute force attack due to trivial user password. Initiated on November 15, 2007 20:47 (GMT+4). Intrusion resulted in an attempts to break other systems in the Internet from the attacked host. Resolved in cooperation with foreign ISPs and CERTs.

16. Conclusion

Hackers and cyber terrorists are launching network attacks with increasing frequency and sophistication. With the increased number of threats to networks such as worms, viruses and clever hackers, security can no longer be viewed as an option. The traditional approach to security - namely a firewall combined with an anti-virus - is incapable of protecting us from today's advanced threats.

We can however have much more protected network environment by implementing network security using a layered approach. By selectively installing security measures on different layers even large network can be adequately protected.

Although there probably is no universal recipe as how to achieve full security, the most appropriate is to proceed always in these three steps: 1)Prevention, 2)Detection, 3)Reaction.

It is necessary to 'look out' and where prevention fails and security is compromised, detect the problem fast and effectively and react appropriately to remove it with the least possible consequences.

No one single security measure is a panacea, but a combination of different methods works best. Moreover one should remember that people are the weakest link in network security field. So the time invested into their continuous education will certainly pay off.