Hardening 

Infrastructure Security: System Hardening

Khadija Jradeh and Maysa Abu Jamra

Under the supervision of Dr. Mouhamad Shaito.



**Outline:**

* General Definition
* Operating System Hardening
* File security
* Updates
* Hotfixes
* Service packs
* Patches
* Network Hardening
* Using secure protocols
* Using anti-malware software
* Implementing switch and router security
* Encryption basics
* Wireless network hardening
* Security policies
* User authentication
* Authentication and authorization methods
* Application Hardening
  + Definition
  + Ports Configuration
  + Techniques (E-mail, FTP, and Web servers)
* Bibliography

**System Hardening**

Hardening refers to providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as defense in depth. Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between. Each level requires a unique method of security.

A hardened computer system is a more secure computer system.

Hardening is also known as system hardening.

In [computing](https://en.wikipedia.org/wiki/Computing), **hardening** is usually the process of securing a system by reducing its [surface of vulnerability](https://en.wikipedia.org/wiki/Attack_surface), which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary [usernames](https://en.wikipedia.org/wiki/User_name) or [logins](https://en.wikipedia.org/wiki/Logging_(computer_security)) , and the disabling or removal of unnecessary [services](https://en.wikipedia.org/wiki/Daemon_(computer_software)).

**Blue Team**

A Blue Team is a group of highly skilled individuals who conduct systematic examinations of Information Systems (IS) or products to determine adequacy of security measures, to identify security deficiencies, to predict effectiveness of proposed security measures, and to confirm adequacy of such measures after implementation.

There are various methods of hardening [**Unix**](https://en.wikipedia.org/wiki/Unix) and [**Linux**](https://en.wikipedia.org/wiki/Linux) systems. This may involve, among other measures, applying a [patch](https://en.wikipedia.org/wiki/Patch_(computing)) to the [kernel](https://en.wikipedia.org/wiki/Kernel_(computer_science)) such as [Exec Shield](https://en.wikipedia.org/wiki/Exec_Shield) or [PaX](https://en.wikipedia.org/wiki/PaX" \o "PaX); closing open [network ports](https://en.wikipedia.org/wiki/TCP_and_UDP_port); and setting up [intrusion-detection systems](https://en.wikipedia.org/wiki/Intrusion-detection_system), [firewalls](https://en.wikipedia.org/wiki/Firewall_(networking)) and [intrusion-prevention systems](https://en.wikipedia.org/wiki/Intrusion-prevention_system). There are also hardening [scripts](https://en.wikipedia.org/wiki/Script_(computer_programming)) and tools like [Lynis](https://en.wikipedia.org/wiki/Lynis" \o "Lynis), Bastille Linux, [JASS](http://sun.com/software/security/jass/) for [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)) systems and Apache/PHP Hardener that can, for example, deactivate unneeded features in configuration files or perform various other protective measures.

**Operating System Hardening**

Most computers offer network security features to limit outside access to the system. Software such as antivirus programs and [spyware](http://techterms.com/definition/spyware) blockers prevent malicious software from running on the machine. Yet, even with these security measures in place, computers are often still vulnerable to outside access. System hardening, also called Operating System hardening, helps minimize these security vulnerabilities.

The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by removing all non-essential software programs and utilities from the computer. While these programs may offer useful features to the user, if they provide "back-door" access to the system, they must be removed during system hardening.

Advanced system hardening may involve reformatting the [hard disk](http://techterms.com/definition/harddisk) and only installing the bare necessities that the computer needs to function. The CD drive is listed as the first boot device, which enables the computer to start from a CD or DVD if needed. File and print sharing are turned off if not absolutely necessary and TCP/IP is often the only protocol installed. The guest account is disabled, the administrator account is renamed, and secure passwords are created for all user [logins](http://techterms.com/definition/login). Auditing is enabled to monitor unauthorized access attempts.

While these steps are often part of operating system hardening, system administrators may choose to perform other tasks that boost system security. While both Macintosh and Windows operating systems can be hardened, system hardening is more often done on Windows machines, since they are more likely to have their security compromised.

**File security**

****

Controlling access is an important element in maintaining system security. The most secure environments follow the “least privileged” principle. This principle states that users are granted the least amount of access possible that still enables them to complete their required work tasks. Expansions to that access are carefully considered before being implemented. Law enforcement officers and those in government agencies are familiar with this principle regarding non- computerized information, where the concept is usually termed *need to know*. Generally, following this principle means that network administrators receive more complaints from users unable to access resources. However, receiving complaints from authorized users is better than suffering access violations that damage an organization’s profitability or capability to conduct business.

In practice, maintaining the least privileged principle directly affects the level of administrative, management, and auditing overhead, increasing the levels required to implement and maintain the environment. One alternative, the use of user groups, is a great time saver. Instead of assigning individual access controls, groups of similar users are assigned the same access. In cases where all users in a group have exactly the same access needs, this method works. However, in many cases, individual users need more or less access than other group members. When security is important, the extra effort to fine-tune individual user access provides greater control over what each user can and cannot access.

Keeping individual user access as specific as possible limits some threats, such as the possibility that a single compromised user account could grant a hacker unrestricted access. It does not, however, prevent the compromise of more privileged accounts, such as those of administrators or specific service operators. It does force intruders to focus their efforts on the privileged accounts, where stronger controls and more diligent auditing should occur.

**Updates**

****

Updates for OSes and NOSes are provided by the manufacturer of the specific component. Updates contain improvements to the OS, and new or improved components that the manufacturer believes will make the product more stable, usable, secure, or otherwise attractive to end users. For example, Microsoft updates are often specifically labeled Security Updates. If you have never taken a look at these, they can be viewed at www.microsoft.com/athome/security/update/bulletins/ 200701.mspx. These updates address security concerns recognized by Microsoft, and should be evaluated and installed as needed. In addition, updates may enhance the capability of a function within the system that was underdeveloped at the time the system or application was released. While you may be tempted to rush out and install these updates on all your vulnerable systems, you may want to test their effect first. Updates should be thoroughly tested in non-production environments before implementation. It is possible that a “new and improved” function (especially one that enhances user convenience) may actually allow more potential for a security breach than the original component. Complete testing is a must.

**Hotfixes**

Hotfixes are repair components designed to repair problems occurring on relatively small numbers of workstations or servers. Hotfixes are generally created by the vendor when a number of clients indicate that there is a compatibility or functional problem with a manufacturer’s products used on particular hardware platforms. These are mainly fixes for known or reported problems that may be limited in scope. As with the implementation of updates, these should be thoroughly tested in a non-production environment for compatibility and functionality before being used in a production environment. Because these are generally limited in function, it is not a good practice to install them on every machine. Rather, they should only be installed as needed to correct a specific problem.

**Service Packs**

Service packs are accumulated sets of updates or hotfixes. Service packs are usually tested over a wide range of hardware and applications in an attempt to assure compatibility with existing patches and updates, and to initiate much broader coverage than just hotfixes. The recommendations discussed previously also apply to service pack installation. Service packs must be fully tested and verified before being installed on live systems. Although most vendors of OS software attempt to test all of the components of a service pack before distribution, it is impossible for them to test every possible system configuration that may be encountered in the field, so it is up to the administrator to test their own. The purpose is to slow or deter com- promise, provide security for resources, and assure availability.

**Patches**

****

Patches for OSes and NOSes are available from the vendor supplying the product. These are available by way of the vendor’s Web site or from mirror sites around the world. They are often security-related, and may be grouped together into a cumulative patch to repair many problems at once. Since patches are issued at unpredictable intervals, it is important to stay on top of their availability and install them after they have been tested and evaluated in a non-production environment. The exception to this is when preparing a new, clean install. In this case, it is wise to download and install all known patches prior to introducing the machines to the network.

**Using secure protocols**

The security threats are changing and increasing, that’s why administrators should harden the network. One of the possible and important solutions is to use secure protocols as:

1. SFTP: it is better than FTP, used to transfer files and manage their structures using SSH. (The communication is encrypted)
2. HTTPS: used to secure the communication channel between a web browser and a web server.
3. SSH: used to create encrypted communications between devices also to create virtual terminal sessions secured (secure shell)
4. SNMP: version 3 because it is better of the 2 others, and this protocol is used to manage and configure devices from a long distance .
5. TLS: used to encrypt online communications.
6. IPsec: use multiple methods to authenticate the extremities of the communication channels.

**anti-malware software**

First, what is an anti-malware software?

* Antimalware software protects against infections caused by many types of malware (viruses, spyware, worms..)
* The terms “antivirus software” and “antimalware software” are used as synonyms but the vendors like to differentiate the two terms. [1]

We have three main options when using anti-malware software:

1. Host-based anti-malware:

The application is installed on our devices.

**Advantage:** easily tuned to the needs of the individual host

**Disadvantage**: requires the user to keep it up to date

1. Network-based anti-malware:

The application is installed on the local network and is served to the clients who want it.

**Advantage:** easily administered

**Disadvantage:** harder to tune for the individual hosts

1. Cloud-based anti-malware:

The application is outside of the LAN, it is in the cloud and is served to the clients in the LAN as needed.

**Advantage:** tend to be kept newer than other options

**Disadvantage:** a very small footprint on the local machines

**Implementing switch and router security**

* **HASHING**

*Before talking about the security measures on each of the router and the switch, an important question should be asked , when using a password is not secure ?*

It is when the password is kept in the clear-text and to resolute this problem we need to use a cryptographic process named hashing.

Hash functions are widely used in many aspects of security, such as digital signatures and data integrity checks. They take an electronic file, message or block and generate a short digital fingerprint of the content called a hash value.

Hashing uses algorithms where MD5 and SHA are the most popular .

The hashing algorithm derives a set value from the sensitive data.

a) **Switch port** security measures:

- enable the switch port security

-native VLAN should be changed from its default value

-all active ports should be assigned to non-native VLANS

-all non active ports should be assigned to an unused non-native VLANS

-network segmentation: VLANS CREATED

-Mac address filtering(specific mac @ connect to specific ports)

-DHCP snooping(only allow responses from administrator defined switch port )

-ARP inspection works with DHCP snooping to prevents the ARP poisoning. All ARP requests are compared to the ARP table which is on the DHCP server

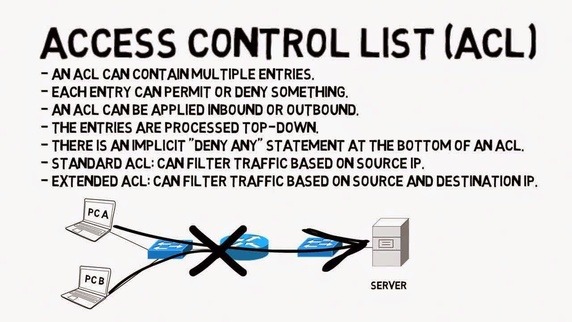
b) **Router port** security measures:

An ACL (Access List) is a set of rules that filter the flow on a network traffic. These rules are based on ip@,protocols...

An ACL is a router configuration script that controls whether a router permits or denies packets to pass based on criteria found in the packet header.

To harden a router each interface should have at least one ACL active on It.

When the packet arrives, we begin with the first rule in the ACL and if it matches the rule , the rule is enforced.

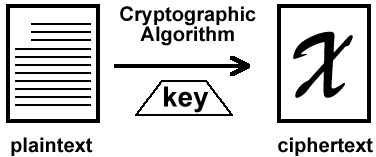
**

**Encryption basics**

Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone expect authorized parties. [2]

An encryption process has a corresponding decryption process, which is used to reverse the encrypted data (cipher text) back to its original content(plaintext).

Each encryption and decryption function requires a key which is formed of a number of binary digits. The more bits it has, the stronger the key is which led us to a better encryption.



There are two basic techniques for encrypting information:

**Symmetric Encryption (secret key encryption):**

The same key is used to encrypt and decrypt the message.

Symmetric algorithms offer more efficiency(fast) but less security.

We have classical cypher which can be monoalphabetic(one by one) or polyalphabetic (the same character can be crypted in a different way) .

Modern cypher can be either BLOCK CIPHER or STREAM CIPHER.

BLOCK CIPHER : work on a block at a time as DES, DOUBLE DES,TRIPLE DES, and AES which is the most used nowadays.

STREAM CIPHER : work on a bit of the message at a time as RC4.

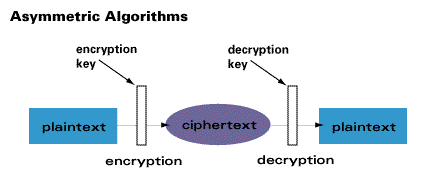
**Asymmetric Encryption (public key encryption):**

It uses two different keys but mathematically linked keys, one public (can be shared with everyone) and one private(must be kept secret).

What one key encrypt the other decrypt and vice versa.

Asymmetric algorithms are more computationally resource intensive but also more secure.

RSA is the most widely used asymmetric algorithm, partly because both the public and private keys can encrypt a message, the opposite key from the one used to encrypt a message is used to decrypt it.



**Wireless network hardening**

There are steps that can be taken to insure that even if the network traffic is captured, it cannot be read:

1. Mac address filtering: limiting which devices can connect to the wireless network. If an unknown device want to connect to this wireless it cannot. This technique can be effective but it is hard to manage.
2. Using the wireless security protocols:

-WEP: Uses a 40-bit per 128-bit encryption key and the RC4 algorithm. It uses a pre-shared key as a password to authenticate users. It is difficult to configure and is easily broken.

-WAP: Uses PSK and RC4 algorithm but is better than WEP.

It introduced temporal key integrity protocol which generates a new security key with a strength of 128 bits or greater for every packet but it can be also cracked .

-WAP2: The most significant enhancement of the WPA2 over WPA is the use of AES algorithm for encryption. The security provided by AES is sufficient. It is good enough to protect your secrets as well.

**Security policies**

The security policies goes far beyond the simple idea of “keep the bad guys out” .

Security policy is a document which is written at the upper layers of management in an organization. It establishes what is allowed or not allowed on a network and allows the administrator to put security measures (use of password, web browser habits).



**User authentication**

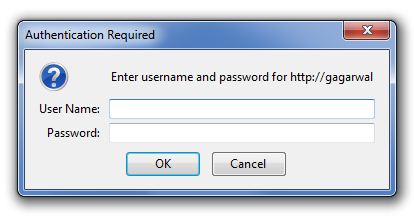
Users and devices allowed on the network should have a strong authentication:

In authentication, the user of computer has to prove its identity to the server, it can be done in one of these ways:

-by what users know: username and password

-by what users are: through biometrics (fingerprint)

-by what users have: through a security token

These factors can be used in combination to increase security.

**Authentication and authorization methods**

Authentication and authorization methods can be done in several ways:

* PAP: when you enter your username and password, they are sent in clear text format . PAP is subject for numerous attacks
* CHAP: when you enter a username and a password, it authenticates through a 3-way handshake process. The resource issues a challenge: what is the hashed values of the username and password?

The user’s device sends a hashed value to the resource device which evaluates the hashed values and either accepts or rejects the connection.

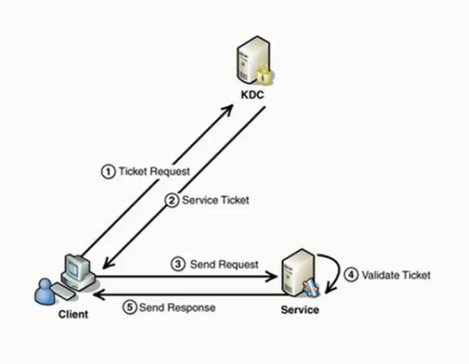
-MS-CHAP: same as CHAP but used only by Microsoft

-EAP (Extensible authentication protocol):

It is a specification that details over 100 separate methods. One of these methods is Kerberos.

What is Kerberos?

* It is an authentication protocol which uses TCP or UDP protocol by default.
* When we use it?
* It works well in environments that have a lot of clients
* How it works?
  + - The KDC (Key Distribution Center) is the main component of Kerberos and it has two parts: AS(authentication server ) and TGS (Ticket-granting server)
* When the user enters his name and password, the hash of these last two is sent to the AS.
  + - * If it likes the hash, it responds with a TGT (ticket granted ticket) and a timestamp.
* The client send the TGT to the TGS.
* The TGS responds with a server ticket (token)
* The token let the user access specific resources
* While TGT still valid, the TGS will grant authorization by issuing a new token.



**Application Hardening**

Applications are the most difficult parts of an IT infrastructure to secure because of their complexity and because they often need to accept input from a variety of users. Here are guidelines to lowering the risk of a system intrusion because of an application flaw:

 Assume all installed applications are flawed—don’t rely on the security programmed into them.

 Physically remove from the system all applications not being used.

 Use firewalls, content filters and OS user authentication features to restrict access to the application, and provide access only to those who absolutely must have it.

 Update all applications to the latest patches when security bulletins are released.

 Internally developed applications need to be code-reviewed for security weaknesses. Consider an external security review for critical applications.

 Externally facing Web applications are high-risk applications because they are a bridge between the outside world and internal customer databases. Be sure to add code that can block or otherwise safely deal with all of the following hostile inputs: missing page parameters, parameters that are unusually long, parameters will nulls or hexadecimal encoding, parameters with Web browser script blocks (which are used to create server-side scripting attacks), and parameters with quotes and semicolons (likely attempts to send hostile SQL commands through to the database).

 If possible, write applications in languages that run in virtual machines--such as Java, Visual Basic .Net or C#--because they provide an extra layer of security protection. Avoid C and C++ because they make it easy to write applications that allow buffer overflow attacks.

By definition application hardening is a process to changing the default application configuration in order to achieve greater security.

**Closing unnecessary ports**

Ports are used by services and other applications to allow two computers to communicate. These ports are doorways into a client or server. Over the years, attackers have exploited ports to gain access to Windows–based computers. Therefore, if a port is open that is not being used by the computer, the port should be closed to help protect the computer from an attacker.

Many approaches are available for closing these ports. Some are manual and can be time consuming and cumbersome when you consider the number of clients and servers in your organization. The following three other approaches are efficient and provide ease of administration and persistence of the configurations:

* **Windows Firewall**

Windows Firewall is designed to control the inbound and outbound communication of a computer. When you configure Windows Firewall, you have a set list of services that you can allow or deny. These services are associated with ports within Windows Firewall. If you have a special port that is not listed through a service, you can add individual ports and services that can be controlled.

* **Security Configuration Wizard**

The Security Configuration Wizard provides a seamless method for configuring ports for servers. It uses server roles, administrative options, and Windows Firewall to open and close ports to protect the server. Within the wizard, you have the option to add specific UDP and TCP ports, as well as add approved applications. (You need not know the ports that the application uses.) You can apply these port restrictions using the wizard, or you can export the security policy to a GPO for deployment through Active Directory.

**Techniques**

**E-mail**

E-mail servers have their own set of built-in and application-specific vulnerabilities. All e-mail servers are vulnerable to normal attacks that are mounted against their specific OS, but they are also vulnerable to Denial of Service (DoS) attacks, virus attacks, and relay and spoofing attacks that may affect the level of service.

To protect the servers, the OS es and NOS es on the server must be hardened, as well as the e-mail service applications. In e-mail, no systems are immune to attack.

There are many deficiencies in the various versions of e-mail server software such as Send mail for Linux and UNIX, and the Exchange/Outlook platform. Any problems that have been exposed must be investigated, to evaluate the services and functions that should be included in the e-mail service. For example, specific vulnerabilities exist if Hypertext Markup Language (HTML) e-mail is used on a system, both on the e-mail server side and the client side. If HTML e-mail is chosen, arrangements must be made to apply all security patches to client machines, browsers, and servers, to protect against arbitrary execution of code. It is also important to evaluate the messaging and instant messaging capabilities, as the implementation of Internet Message Access Protocol (IMAP) technologies may also expose the network to further risk. Additionally, e-mail servers are constant potential sources of virus attacks, and therefore must have the strongest possible protection for scanning incoming and outgoing messages. Finally, e-mail servers should not have extraneous services and applications installed, and administrative and system access permissions should be tightly controlled to block installation or execution of unauthorized programs and Trojans.

When hardening an e-mail server, it is important to consider the following attack points:

* E-mail relay, which allows unauthorized users to send e-mail through an e-mail server
* Virus propagation; make sure the anti-virus planning and applications are performing correctly
* Spamming, including DoS conditions that exist in response to “flame wars”
* Mail bombing; the practice of flooding the recipients e-mail account with huge amounts of mail
* Storage limitations, to limit DoS attacks based on message size or volume

**FTP Servers**

FTP servers are potential security problems, as they are exposed to outside interfaces, thereby inviting anyone to access them. The vast majority of FTP servers open to the Internet support anonymous access to public resources.  Incorrect file system settings in a server hosting an FTP server allows unrestricted access to all resources stored on that server, and could lead to a system breach. FTP servers exposed to the Internet are best operated in the demilitarized zone (DMZ), rather than the internal network. They should be hardened with all of the OS and NOS fixes available, but all services other than FTP that could lead to breach of the system should be disabled or removed. Contact from the internal network to the FTP server through the firewall should be restricted and controlled through ACL entries, to prevent possible traffic through the FTP server from returning to the internal network.  FTP servers providing service in an internal network are also susceptible to attack; therefore, administrators should consider establishing access controls including usernames and passwords, as well as the use of SSL for authentication.  Some of the hardening tasks that should be performed on FTP servers include:

Protection of the server file system

* Isolation of the FTP directories
* Positive creation of authorization and access control rules
* Regular review of logs
* Regular review of directory content to detect unauthorized files and usage

**Bibliography:**

1. <http://searchsecurity.techtarget.com/definition/antimalware>
2. <http://searchsecurity.techtarget.com/definition/encryption>
3. <http://www.eweek.com/c/a/Application-Development/Application-Hardening-Checklist>
4. Security Study Guide
5. [https://en.wikipedia.org/wiki/Data\_**security**](https://en.wikipedia.org/wiki/Data_security)