Operating System Hardening

Windows-Hardening
Linux-Hardening

Seminararbeit

Ausgewählte Kapitel der IT-Security

Vorgelegt von:
Betül Aras

Personenkennzeichen
1910475038

Abgabe am:
21.11.2022

List of Abbreviations

APMD	Advanced Power Management Daemon
BIOS	Basic Input/Output System
CIS	Center for Internet Security
CVE	Common Vulnerabilities and Exposures
DIS	Defense Information Systems Agency
LILO	Linux Loader
LSM	Linux Security Modules
MFA	Multi-Factor Authentication
PAM	Pluggable Authentication Modules
WSUS	Windows Server Update Services

Keywords

Hardening
Linux Server Hardening
NTLM
Threats and security risks
Windows Server Hardening

Contents

Chapter 1

Introduction

Even with effective security techniques, an unsecure operating system can compromise the security of a whole system. Different levels and profiles of security are provided by various operating system security features. The appropriate degree or essential profile of protection for a system must be selected by the administrator. Windows NT is generally referred to as the most secure commercially available operating system by supporters. Others tend to concur with this view after learning about Unix's numerous and well-known security flaws [VV00].

It is intended that by giving a quick overview of Linux and Windows' security concerns, readers come to the conclusion that both operating systems have worth from a security standpoint and that there is no obvious winner in terms of security.

For instance, typically there are no security measures or checks performed inside the kernel, all kernel components are explicitly trusted, and there are no procedures that separate one element of the kernel from other parts of the kernel. As a result, kernels often do not defend themselves. If the operating system has a security flaw, anyone who is able to exploit it, can take total control of the machine by employing the right software programs. It is challenging to create self-protecting kernels, and performance is frequently severely sacrificed. Nevertheless, both, Linux and Windows operating systems have their advantages and disadvantages and this paper gives an overview of available hardening mechanisms both Linux and Windows operating systems, since both play a significant role in daily living.

Chapter 2

Hardening

Hardening is the process of implementing security measures to increase security. Applying security measures always involves striking the right balance between security and environmental concerns and since the era of "big security" has arrived in our society, the business system of the companies or organizations is now affected by the following issues: firstly, the majority of business systems do not take into account the need for security protection at a future stage of planning and development. Secondly, restarting is necessary for the operating system patch to take effect. The demand for a powerful communication and information system for intelligence, ubiquity, and automation is growing daily as the businesses build a new computer room and expand the size of its private cloud resource pool.

On the basis of the present information security protection system, it is necessary to complete the protection blind spot and improve the protection capabilities of continuous updating. The New Technology LAN Manager (NTLM), for instance, is to disable, but doing so prevents an older, mission-critical system in the organization from being capable of authenticating against Active Directory [Ori22].
The level of risk for managing an Active Directory infrastructure for a federal government agency differs significantly from that of managing an Active Directory environment for a local school district.

Users often and infrequently conduct actions on the system and occupying the desktop with different tasks, such as installations, uninstalls, starting and stopping services, disabling and unable customisation's, etc. The system remains open to exploits and vulnerabilities because of different numerous changes. However, users may ensure a higher level of system security if they regularly assess and prioritise operating system threats [CDS+21]. System hardening, often known as periodic auditing, entails securing the system by lowering risks according to priority.

Everyone in the industry, from the information worker to top management (such as the CEO), is impacted by security. A security breach might possibly disrupt all regular activity and put your organization's operations on hold. Lack of security is a genuine issue for enterprises.

Cybersecurity attacks has a $3 trillion annual consequence on missed productivity and growth, according to recent research from McKinsey, the Ponemon Institute [Pon], and Verizon [VCI]. The typical security breach costs $3.5 million. Similar to any other crime, the earlier a possible attack is discovered, the more or earlier a step of mitigating any security risk occurs [Ori22].

2.1 Security Baselining

Security baselining is the method of putting a minimal set of guidelines in place and configurations for your environment e.g. establishing a minimal Windows device setup [Dun20]. The creation of a baseline offers a minimally defined norm that will assist assuring a better secure environment if the organisation or the organisational institution deploys systems and devices.

Baselines can range from checklists or spreadsheets where someone uses to ensure sure the predetermined security controls have been implemented to a taken snapshot or picture that is already preloaded with the predefined security rules, depending on the size of your business.

An aspect of the baseline, it is important to confirm that policies, standards, and processes are in place, are clearly defined, and have received the approval of the leadership and all other stakeholders who are responsible for e.g. data protection. It is essential to have these specified for security, compliance, and auditing reasons. To begin, policies for the firm are to be established and defined. The baselines are then to be constructed using the standards as the framework.

After these baselines are established, policies and procedures is to be developed to apply the baselines and support the achievement of the ultimate result. In the long run, deploying baselines without clear policies, procedures, and a framework is not presumed as effective and leaves the business open to risk. Additionally, having these foundations in place provides a platform with ensuring leadership participation and sign-off, which sends a consistent message to the company about the significance of each associate in its success.

2.2 Security Policies, Standards and Procedures

The first level of official documentation for an organization's security program is the so-called security policy, which is a must and to be followed. The leadership team's approval and support are necessary for the policies, which are an essential part of the overall security program, to succeed. There is no clear connection between the policies and the organization's technologies or solutions; they are highly broad and wide [Dun20].

It is strongly advised to start with the fundamentals if the business does not already have any rules in place that pertain to, for example, Windows security. In order to protect the devices, at the very least, the following few examples are to be mentioned in a policy [Dun20]:

- Security updates
- Firewall
- Encryption
- A password policy, multi-factor authentification (MFA) and biometrics

A policy that demands that all systems be maintained up to date with the most recent security updates is an example.

Policies are followed by standards, which are obligatory and describe the specifics of each policy. In addition to providing details on the technology to be used, standards help maintain consistency within an organization.
A few examples of standards regarding windows server for the proposed elements described in the preceding section include the following [Dun20]:

- Windows Update for Business is to be used to setup all Windows 10 computers, while Windows Servers use either Windows Server Update Services (WSUS) or Azure Update Management. The business use case will specify and store update schedules.
- On all Windows end user devices and servers, the Windows firewall is to activate and set up. The connection requirements is to be defined.
- Using BitLocker and/or Azure Disk Encryption, all Windows servers and end user workstations is to be encrypted.
- PINs and Windows Hello biometrics is to install, and accounts require utilizing passwords with a minimum of 12 characters. Passwords requisite updates yearly and contain capital, lowercase, number, and special characters.

The detailed instructions including a step-by-step guidance required to complete a repetitive operation or process are known as procedures. These collection or set of guidances are meant to help with the implementation of the stated policies, standards, and as well as guidelines to achieve a specific aim.

Procedures requisite updates periodically as technology and software versions advance. A third-party tool is also an option in the aim of being more organized and completing procedures. One instance is a program called Nintex Promapp [Pro], which aids in documenting and sharing your company's procedures [Dun20].

The following four steps are an illustration of a procedure:

1. Set up a new Windows 10 device.
2. Verify that the device is provided with internet connection.
3. Verify the configurations of the device, the device setups, and so on.
4. Verify the device's compliance.

The figure 2.1 shows an overview of policies, standards, procedures and baselines and how they are linked to one another.

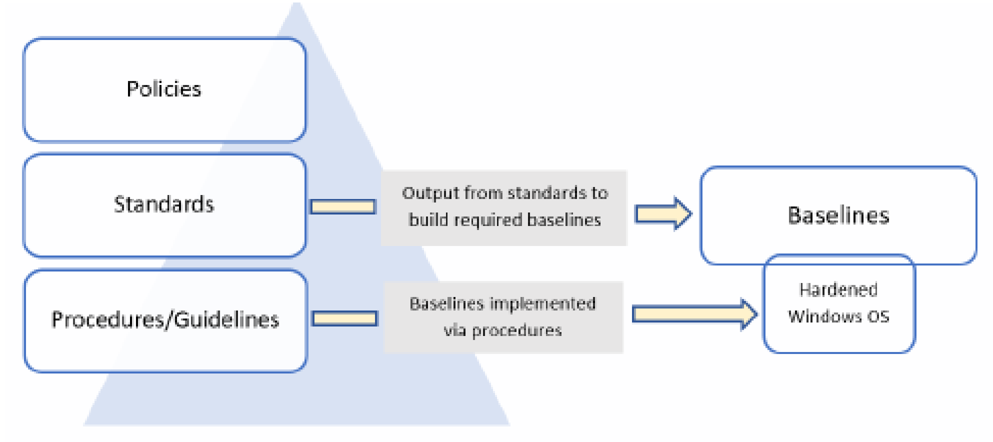

Policies
Standards
Output from standards to build required baselines
Baselines
Procedures/Guidelines
Baselines implemented via procedures
Hardened Windows OS

Figure 2.1: Policies, standards, procedures, and baselines [Dun20]

Chapter 3

Linux Hardening

The Linux kernel and operating system are also complicated and difficult to setup. In reality, Linux systems are incredibly adaptable, and even little configuration adjustments can have a big impact on security. As a result, not all security exposures and vulnerabilities are immediately apparent, and failing to consider the overall effects of modifying configuration items might result in unintended exposures.
Additionally, security in Linux systems is dynamic. The system is not always secure once it has been secured. It is true that a system loses security the longer it is in use. This occurs as a result of operational or functional changes that expose systems to risks or as a result of new vulnerabilities being found in software packages and applications. The process of system security is continuous and active [At22].

Finally, many distributions provide a suggested default set of packages, programs, and settings when they are bundled or setup. This setting often depends on the author or vendor knowing what the distribution's end user needs. For example, Red Hat is preconfigured to utilize Pluggable Authentication Modules (or PAM) for a number of authentication procedures, which is generally advantageous and improves the potential security of the system. However, occasionally this preconfiguration introduces security flaws or is not well thought out in terms of security.

For instance, the vendor could install, configure, and launch apps or services to make it simple for users to set up the system. Red Hat, for instance, when using the default installation settings, automatically configures and launches Sendmail. It is clear that Linux has several security-related advantages over Windows. The following are a few of them [Tev18]:

- Unlike Windows, Linux was created from the ground up to be a multi-user operating system. Therefore, user security on a Linux system is higher.

- Windows is significantly more vulnerable to virus and malware attacks than Linux is.

- Linux provides a better way to separate privileged users from administrative users. This makes it slightly more difficult for hackers as well as for users to unintentionally infect a Linux machine with something dangerous.

- Compared to Windows, Linux is far more resistant to virus and malware infections.
- SELinux and AppArmor are built-in techniques in some Linux distributions like Red Hat and CentOS and SELinux, , that stop intruders from taking over a system.
- Linux is a free and open-source operating system. This makes it possible for anyone with the knowledge to audit Linux code to look for flaws or backdoors.

However, despite these benefits, Linux is still a human invention like everything else. So, it is not perfect. Following the news in the IT sector in the last few years, there is at least a few incidents about how hackers have compromised Linux systems [At22].

While it is true that Linux is not particularly vulnerable to virus infections, there have been multiple reports of attackers planting other sorts of malware on Linux servers. Among these cases are [Tev18]:

- **Botnet malware** forces a server to engage a botnet directed by a remote attacker. One of the most well-known events was the connection of Linux servers to a botnet that performed denial-of-service attacks against other networks.
- **Ransomware** is a type of malware that encrypts user data until the server owner pays a ransom charge. However, even if the cost is paid, there is no assurance that the data can be retrieved.
- **Cryptocoin mining software** utilizes more energy and makes the server's CPUs work harder when it is installed. The accounts of the attackers who installed the program receive any Cryptocoins that is mined.

There have been several breaches that did not require malware, such as when attackers discovered a way to steal user passwords, credit card data, or other confidential information.

3.1 Existing Tools and Limitations

System administrators and security teams can record actions carried out, for example, on a Linux system and send them to a central place for storage and analytics, relying to a rather limited set of open source tools.
These technologies often include Security Investigation and Event Management (SIEM). System logs or Auditd are two tools that may be used to gather records of operations carried out on Linux systems.[ASS$^+$22].

Linux system logs: By default, Linux systems record all system activity for debugging purposes rather than necessarily to help future security investigations. The following logs are provided on Linux systems to assist users comprehend the various types of operations taking place.

- Syslog and messages : global system activity, including startup messages.
- Auth.log and secure : Security modules like PAM (Pluggable Authentication Module).
- Kern.log : kernel events, errors and warning logs.
- Cron : information about running cron jobs.
- Application specific logs : example /var/log/apache for web server logs.

Logs from the auditing daemon Auditd provide for verbose logging and even the recording of individual syscall usages by the system administrator. Numerous configuration factors, both at the operating system level and the application level, are required for the Linux operating system to be secure.

3.2 Secure Booting and Boot Loaders

In particular, controls including users and passwords make it easy for an attacker with physical access to the system to prevent many of its inherent security measures. They can also easily reboot the machine or alter the configuration of boot loader or init process, which affects which services are launched at boot and in what order.

Two significant issues can arise from attackers who are able to reboot the machine. The first is that someone who has access to how the device boots into a Linux machine can gain a significant amount of access to it. The second big issue is that a major Denial of Service attack takes the machine offline.
Therefore, it is necessary to carefully restrict access to the ability to reboot the system, how users interact with the boot loader, and the kernel they boot into.

The Linux Loader (LILO) or Grub are the two boot loaders that the majority of Linux systems utilize. When the system is started or restarted, these boot loaders decide which kernel will boot and manage the boot images. They are loaded after the Basic Input/Output System (BIOS) has instantiated the system and typically waited for a predetermined amount of time (typically between 10 and 30 seconds, but overriding is possible) before choosing a kernel to boot into; if no action is taken, they default to a predetermined kernel and boot into that.

Older kernels are frequently left on computers and in boot loader menus. There is a chance that an attacker boots into an outdated kernel that contains a security hole, giving them access to the machine. When upgrading kernels, cleanup is required.

If an attacker has already gained physical access to the system, both boot loaders, LILO and Grub, are implicitly unsafe. For instance, both LILO and Grub by default support single-user mode booting. Without needing to input the root password, the single-user mode provides root rights.

The boot loader's command lines also allow for the input of a number of other arguments, which can give an attacker possibilities to compromise the machine. But this can be avoided by using passwords to encrypt LILO and Grub, and in the next chapter it is demonstrated how to achieve that for both boat loaders [Tur05].

3.2.1 Securing LILO with a Password

A password is then to be specified in the lilo.conf file to stop LILO from enabling unrestricted booting, however selecting a non-default boot item, adding options to the boot items, or booting into single-user mode are also allowed.

```
prompt
timeout=50
default=linux
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear
password=secretpassword
restricted

image=/boot/vmlinuz-2.4.18-14
          label=linux
          intitrd=/boot/initrd-2.4.14-14.img
          read=only
          append=”root=LABEL=/”
```

The restricted and password options are the two key elements to pay close attention in the configuration above [Tur05]. These are not included by default in the lilo.conf file; they must be applied separately. When the machine is first initiated, the password option enables the specification of a password that must be provided before it is permitted to boot.

A password that is sufficiently safe is to utilize in place of the term secretpassword in the figure above. Unfortunately, this password is put to the lilo.conf file in clear text, making it accessible to anybody with access to the file (Although it is recommended to only be available to those with root permissions).

The restricted option modifies the password option's behavior. With restricted set, LILO only asks for a password if the boot loader command line arguments are provided. For instance, if someone attempted to provide the boot loader command line argument single (to enter single-user mode), it requires a password.
With a specific kernel image statement, the password and restricted options can also be specified.

In this manner, it is possible to secure a specific kernel image or offer unique passwords for every kernel image.

The restricted option is used in the example below, making it mandatory to enter a password in order to attempt to boot this kernel image [Tur05]:

```
image=/boot/vmlinuz-2.4.18-14
        password=secretpassword
        label=linux
        initrd=/boot/initrd-2.4.18-14.img
        read-only
        append= "root=LABEL=/"
```

Running the lilo command to update LILO settings is required whenever the lilo.conf file is modified [Tur05]:

```
puppy# /sbin/lilo
```

The last step is to make sure that the lilo.conf file has the necessary ownerships and permissions so that only those who are permitted are able to read the password [Tur05]:

```
puppy# chown root:root /etc/lilo.conf
puppy# chmod 0600 /etc/lilo.conf
```

3.2.2 Securing Grub with a Password

Likewise LILO, Grub has security flaws which let anybody with access at boot time modify the boot configuration or boot into single-user mode. The available Grub password security is slightly more extensive than LILO's and depends on creating an MD5-encrypted password to protect the boot menu and startup entries. Due to the MD5 encryption, the password cannot be obtained by merely reading the /etc/grub.conf configuration file for Grub.

```
puppy# grub
grub> md5crypt
Password: ********
Encrypted: $1$2FXKzQo$I6k7iy22wB27CrkzdvPe70
grub>quit
```

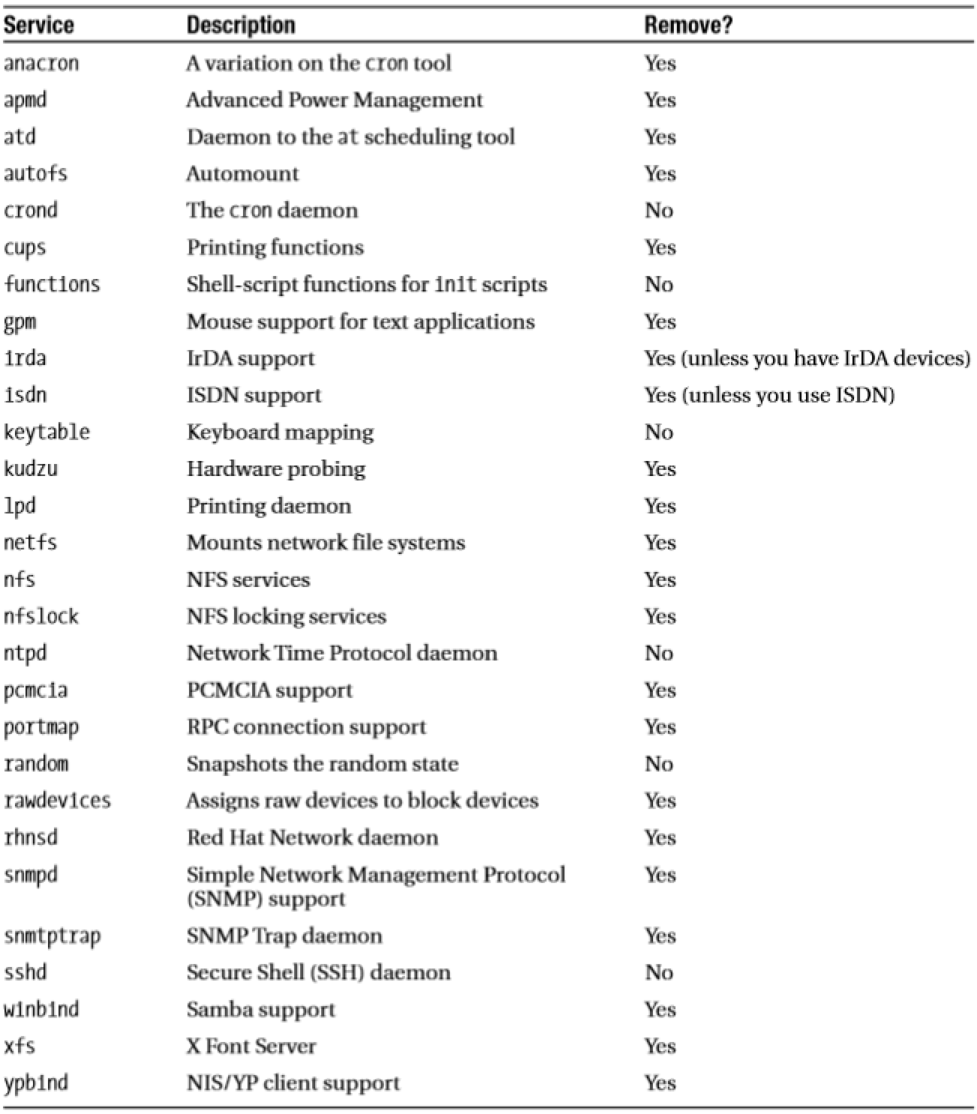
First, the Grub shell is entered, the md5crpyt option is run, and a password prompt appears. An MD5 hash of the password is then generated and shown on the screen as shown above [Tur05].
The password is to be copied once it has been MD5-encrypted and added to the grub.conf configuration file [Tur05]:

```
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
password --md5 $1$2FXKzQo$I6k7iy22wB27CrkzdvPe70
title Red Hat Linux (2.6.7)
        root (hdo,0)
        kernel /vmlinuz-2.6.7 ro root=LABEL=/
        initrd /initrd-2.6.7.img
```

It is possible to add the password —md5 option to a file and provide the generated MD5 password. Now, unless p is typed and the necessary password is entered, it is not possible to interact with the Grub boot menu when the computer is rebooted.

3.3 Starting Services

The majority of systems come with a lot of services that launch when the system boots. Naturally, some of these are essential to the operation of the system, while others are made to launch programs that operate on the system, like Sendmail or Apache. Many of the others, however, either launch services that are not required or compromise the system's security.



Service	Description	Remove?
anacron	A variation on the cron tool	Yes
apmd	Advanced Power Management	Yes
atd	Daemon to the at scheduling tool	Yes
autofs	Automount	Yes
crond	The cron daemon	No
cups	Printing functions	Yes
functions	Shell-script functions for init scripts	No
gpm	Mouse support for text applications	Yes
irda	IrDA support	Yes (unless you have IrDA devices)
isdn	ISDN support	Yes (unless you use ISDN)
keytable	Keyboard mapping	No
kudzu	Hardware probing	Yes
lpd	Printing daemon	Yes
netfs	Mounts network file systems	Yes
nfs	NFS services	Yes
nfslock	NFS locking services	Yes
ntpd	Network Time Protocol daemon	No
pcmcia	PCMCIA support	Yes
portmap	RPC connection support	Yes
random	Snapshots the random state	No
rawdevices	Assigns raw devices to block devices	Yes
rhnsd	Red Hat Network daemon	Yes
snmpd	Simple Network Management Protocol (SNMP) support	Yes
snmtptrap	SNMP Trap daemon	Yes
sshd	Secure Shell (SSH) daemon	No
winbind	Samba support	Yes
xfs	X Font Server	Yes
ypbind	NIS/YP client support	Yes

Figure 3.1: Starting Services for Red Hat and Debian [Tur05]

When determining whether to start any of the services shown in the picture above, many of them function when rational thinking or common sense is used. The figure above refers to Releases of Red Hat 9, Red Hat Fedora Core, Red Hat Enterprise Linux 3, and Debian Woody 3 [Tur05]. For instance, while the Advanced Power Management Daemon (APDM) daemon is frequently used on laptops to offer the necessary power management functions, it is uncommon to see it operating on a production server.

Chapter 4

Windows Hardening

Misconfigurations weaken a system's security by creating vulnerabilities that are frequently hard to find. According to a recent research [CDF18], ignorance and lack of knowledge are the main causes of security misconfigurations from the operators' point of view. Utilizing already-existing security-configuration manuals is one method for overcoming the lack of knowledge. Each rule describes why it should be used and what parameter should be changed to increase system security, as shown in figure 4.1.

```
## /rule
The number of allowed bad logon attempts must be configured to three
↪   or less.
## /description
The account lockout feature, when enabled, prevents brute-force
↪   password attacks on the system. The higher this value is, the
↪   less effective the account lockout feature will be in protecting
↪   the local system. The number of bad logon attempts must be
↪   reasonably small to minimize the possibility of a successful
↪   password attack while allowing for honest errors made during
↪   normal user logon.
## /implementations/0/description
Configure the policy value for Computer Configuration >> Windows
↪   Settings >> Security Settings >> Account Policies >> Account
↪   Lockout Policy >> "Account lockout threshold" to "3" or fewer
↪   invalid logon attempts (excluding "0", which is unacceptable).
```

Figure 4.1: An illustration of a rule from a security configuration manual for Windows [SGP20]

The Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA) are two well-known distributors of such manuals and these guidelines may be used by organizations and businesses like Siemens to protect their systems.

Since organizations like Microsoft make a significant effort to design their systems safely by default, one could be compelled to disagree that we do not require security configuration. Certainly, these businesses make significant investments in security, but security is only one issue among many, including usability. Assuming that there is an option of a handy setting that is convenient for most users but presents a little security risk. The organisation may be tempted to configure it to be activated by default, but security-conscious users might remove it. There is a similar case for the data gathering settings. They provide expertise and knowledge to the businesses so they may enhance their services, which benefits all customers. So, the businesses may be persuaded to turn on data gathering settings by default. Customers with strict security needs, however, disable them to lessen the chance that private information may unintentionally leak through the data collecting. As a result, security-conscious users help make their systems more safe by using security setup instructions from independent organisations.

4.1 Windows Security Baselines

Microsoft includes suggested settings for hardening Windows systems in its service offerings for Windows security baselines. The following are considered by the Windows security baselines [Dun20]:

1. Windows 10
2. Windows Server
3. Office 365 ProPlus

There are more than 3,000 GPO settings for Windows 10 and more than 1,800 for Internet Explorer 11 to offer a better understanding of the complexity of securing Windows. This demonstrates the necessity of utilizing specified baselines to aid harden Windows devices.The following list of Microsoft tools are the ones that are most frequently used to implement these baselines [Dun20]:

1. Microsoft Intune
2. GPOs
3. Microsoft Endpoint or System Center Configuration Manager

4.1.1 Implementing a Baseline - CIS

Once the organization has preferred which baseline controls to implement, it is required to analyze the controls, deploy them throughout the whole organization, and integrate them into the ongoing process. Moving forward with Center for Internet Security (CIS) benchmark [fIS22], it is necessary to download and modify according to the organisation's requirements and needs. To make deployment simpler, CIS can also choose to purchase hardened images. The procedures below must be taken in order to download the most recent CIS benchmarks [Dun20]:

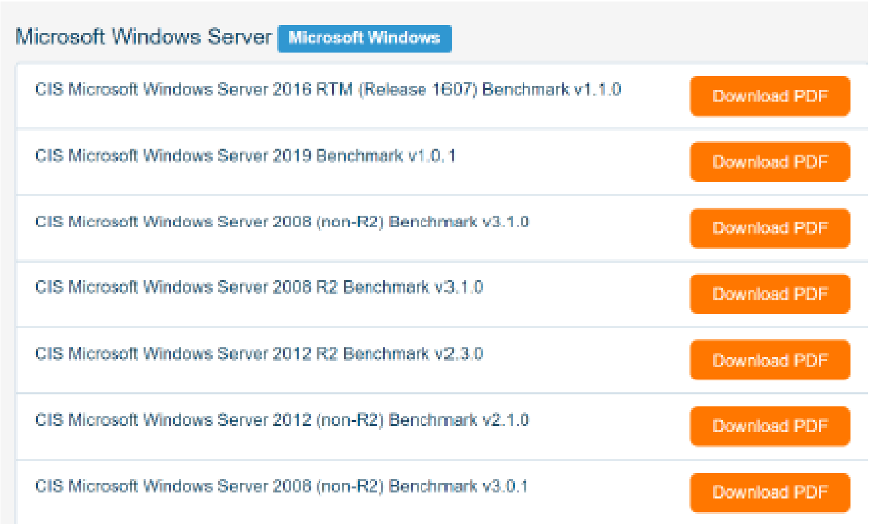
1. Open a browser and navigate to https://www.cisecurity.org/.
2. Click on Cybersecurity Tools.
3. Click on Download under CIS Benchmarks.

4. Enter the required information, agree to the terms, then click on Get Free Benchmarks Now

5. Go to your mailbox and look for an email from CIS (check your Junk email folder too).

6. Open the email and click on Access PDFs. You will be provided with a list of all the available CIS benchmarks in PDF format.

7. Scroll down and you will see the Windows Server benchmarks:



Microsoft Windows Server

CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.1.0

CIS Microsoft Windows Server 2019 Benchmark v1.0.1

CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.1.0

CIS Microsoft Windows Server 2008 R2 Benchmark v3.1.0

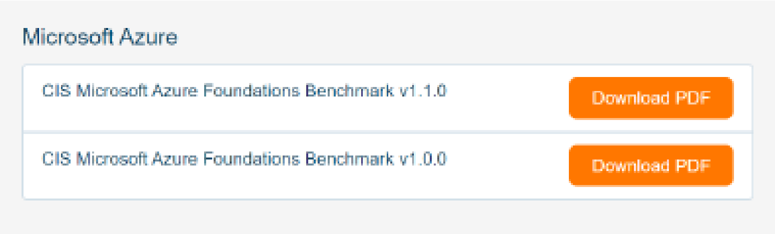
CIS Microsoft Windows Server 2012 R2 Benchmark v2.3.0

CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.1.0

CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.0.1

Figure 4.2: The CIS Benchmarks PDF [Dun20]

8. Keep scrolling down and you will also see the Azure benchmarks:



Microsoft Azure

CIS Microsoft Azure Foundations Benchmark v1.1.0

CIS Microsoft Azure Foundations Benchmark v1.0.0

Figure 4.3: The CIS Benchmarks PDF [Dun20]

9. In addition, there are many more Windows-specific benchmarks for specific roles, such as IIS, SQL, Exchange, and so on.

10. Once you have downloaded the PDFs, follow and implement the recommendations on them to strengthen your systems.

Chapter 5

Conclusion

This seminar paper provides an overview beginning with the term of hardening in the information technology and starts with the concepts of baselining in terms with Linux and Windows operating systems to comprehend its importance and its role within the overall security program. In conclusion, an operating system is not be considered as a person's only line of defense. Despite using decent security concepts and mechanisms, neither Windows nor Unix are sufficient. It is the responsibility of the individual or organisations to be informed about security-related news releases and freshly issued updates. The individual or corporation is to remain prepared as possible to combat these constant threats by being aware of the security risks to be able to minimise them. Although developing a security framework and implementing procedures with complete compliance is ideal, exceptions need to be taken into consideration. It is advised that the organisation additionally maintain a risk registry that lists all the programs and systems that do not adhere to the established policies and regulations. The register lists every risk and rates the implications or seriousness of each risk as well as its possible effects on the business. In addition to being considered from a security angle, these implications should also identify any potential financial and legal consequences in the event that the risks were taken. These dangers must be made apparent to the management, who also authorises their acceptance.

Appendix A

List of contents

List of Figures

List of Tables

Bibliography

[ASS+22] Shubham Agarwal, Arjun Sable, Devesh Sawant, Sunil Kahalekar, and Manjesh K. Hanawal. Threat detection and response in linux endpoints. In *2022 14th International Conference on Communication Systems and Networks (COMSNETS)*, pages 447–449, 2022. 7

[At22] Cybersecurity Researchers At. Linux devices 'increasingly' under attack from hackers, warn security researchers — zdnet. *Cybersecurity Researchers*, 2022. 6, 7

[CDF18] Kevin Borgolte Constanze Dietrich, Katharina Krombholz and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. *In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018. 13

[CDS+21] Emmanuel Casseau, Petr Dobiáš, Oliver Sinnen, Gennaro S. Rodrigues, Fernanda Kastensmidt, Alessandro Savino, Stefano Di Carlo, Maurizio Rebaudengo, and Alberto Bosio. Special session: Operating systems under test: an overview of the significance of the operating system in the resiliency of the computing continuum. In *2021 IEEE 39th VLSI Test Symposium (VTS)*, pages 1–10, 2021. 2

[Dun20] Mark Dunkerley. *Mastering Windows Security and Hardening.* 2020 Packt Publishing, 2020. 3, 4, 5, 14, 15, 18

[fIS22] CIS Center for Internet Security. Our mission is to develop and promote timely best practice solutions, www.cisecurity.org. *CIS*, 2022. accessed: 2022-11-19. 14

[Ori22] Thomas Orin. Microsoft windows server 2019 inside out - windows server 2019 (inside out). *Windows Server 2019 (Inside Out)*, pages 581–639, 2022. 2, 3

[Pon] Institute Ponemon. www.ponemon.org. Accessed: 2022-11-02. 3

[Pro] Promapp. Business process management - www.nintex.com. Accessed: 2022-11-07. 4

[SGP20] Patrick Stöckle, Bernd Grobauer, and Alexander Pretschner. Automated implementation of windows-related security-configuration guides. In *2020*

35th IEEE/ACM International Conference on Automated Software Engineering (ASE), pages 598–610, 2020. 13, 18

[Tev18] Donald Tevault. *Mastering Linux Security and Hardening.* 2018 Packt Publishing, 2018. 6, 7

[Tur05] James Turnbull. *Linux Hardening.* Springer-Verlag New York, 2005. accessed: 2022-11-19. 9, 10, 11, 12, 18

[VCI] Institute Verizon Communications Inc. www.verizon.com. Accessed: 2022-11-02. 3

[VV00] J. Viega and J. Voas. The pros and cons of unix and windows security policies. *IT Professional*, 2(5):40–47, 2000. 1