	Questo comportamento deve essere necessariamente disabilitato, dato che tra i "Safe Files" ci sono immagini e file di installazione di applicazioni, oltre che video, immagini, file archivio e testo. Tali file vengono aperti nel contesto del sistema operativo anziché in un contesto isolato nel browser e dunque rappresentano gravi rischi per la sicurezza del sistema. La funzionalità è configurabile nelle preferenze generali di Safari.

Plug-ins di Safari	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	A partire da Safari 10, è possibile abilitare o disabilitare i plug-in in base a uno specifico sito oltre che globalmente (come in passato). Per ovvi motivi di sicurezza, è necessario, quindi, con Safari versione 10 o successivo, disabilitare la configurazione che abilita globalmente i plug-in, optando invece per una configurazione in cui i plug-in sono globalmente disabilitati. All'accesso a un sito che richiede un certo plug-in, Safari chiederà all'utente se abilitare o no il plug-in per quel sito.

Java Virtual Machine	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Attacchi all'integrità dei sistemi (software e configurazioni). - Accesso non autorizzato alle informazioni.
Contromisure	Apple, in passato, inseriva Java come parte del sistema operativo "core", ma sfortunatamente non fornisce più i relativi aggiornamenti rilasciati da Oracle. La versione più recente di Java, rilasciata da Apple, contiene peraltro numerosi difetti e vulnerabilità e pertanto non deve essere registrata come default runtime delle Applet Java. È necessario quindi disinstallare del tutto Java se non in uso, o altrimenti assicurarsi di aver installato la versione più recente fornita da Oracle.

5.2.12 Sicurezza di Linux

Il primo passo necessario per l'hardening di un server GNU/Linux è determinare la funzione che il server è chiamato a svolgere, e che stabilisce quali servizi necessariamente devono essere installati. Per esempio, se il server è usato come server web, si potrebbero installare i servizi Linux, Apache, MySQL e Perl/ PHP/ Python etc. Se invece il server viene utilizzato per i servizi di directory, le uniche applicazioni e servizi che dovrebbero essere disponibili e pertanto installati sono quelli necessari per il compito prestabilito. Non dovrebbe essere installato altro per due principali motivi:

1. L'installazione di software extra o l'esecuzione di servizi extra potenzialmente espone il sistema a inutili vulnerabilità. Ad esempio, se si installa e si usa un servizio Lightweight Directory Access Protocol (LDAP) su un server per servizi di directory, sia il sistema operativo che LDAP dovrebbero essere regolarmente aggiornati con le relative patch di sicurezza e bug fixing. Ciò sarebbe necessario anche se si installasse qualsiasi altro software, a prescindere dal fatto che questo venga usato o meno, e tale software dovrebbe essere sottoposto comunque a regolari aggiornamenti. La

semplice presenza sul server di software non necessario, fornisce ad un attaccante un'altra via d'accesso al sistema.

2. Installare software extra su un server significa che qualcuno potrebbe essere tentato di usare il server per qualcosa di diverso dall'uso previsto. L'utilizzo del server per compiti diversi da quello principale sottrae risorse al compito per cui è destinato e nel contempo lo espone a potenziali minacce.

In linea generale, le pratiche più comuni indicate nelle diverse linee guida di hardening dei sistemi GNU/Linux, includono:

- la cifratura dei dati nelle comunicazioni,
- l'esclusione di protocolli insicuri che trasportano informazioni o password in chiaro,
- la riduzione della presenza di software non necessario sul sistema,
- la disattivazione di file eseguibili/binari o directory indesiderati con permessi speciali come SUID e SGID,
- il mantenimento dello stato di aggiornamento del sistema operativo, con particolare riguardo alle patch di sicurezza,
- l'utilizzo di estensioni di sicurezza come valore aggiuntivo,
- l'adozione di SELinux come sistema di controllo accessi,
- l'uso di account con password molto robuste,
- il regolare cambiamento delle password e il non riutilizzo di password recenti,
- il blocco degli account che presentano numerosi errori di login,
- l'impossibilità di utilizzare password vuote,
- l'hardening del protocollo e dei servizi SSH,
- la disabilitazione dei servizi non necessari,
- il rafforzamento in termini di sicurezza dei percorsi /tmp, /var/tmp e /dev/shm,
- l'occultazione delle versioni del BIND DNS server e dell'Apache server,
- l'hardening del sysctl.conf,
- l'installazione di Root Kit Hunter e ChrootKit Hunter,
- la riduzione al minimo delle porte di rete aperte nel sistema,
- la configurazione del firewall di sistema,
- la separazione delle partizioni in modo da rendere il sistema maggiormente sicuro,
- la disattivazione di file binari indesiderati,
- la gestione dei log del sistema; con l'esecuzione del mirroring dei log su un server di log separato,
- l'installazione di Logwatch con una revisione giornaliera delle e-mail inviate da tale sistema,
- l'utilizzo di sistemi di rilevamento di attacchi di forza bruta e delle intrusioni,
- l'installazione di Linux Socket Monitor,
- l'installazione di Mod_security,
- l'hardening dell'installato Php,
- la limitazione per gli account ad accedere solo a ciò di cui questi hanno bisogno,
- l'adeguata gestione dei backup,
- la sicurezza fisica del server.

In informatica, solitamente il termine hardening identifica il processo di sicurezza atto a ridurre in un sistema la superficie vulnerabile. Il suo obiettivo principale è quello di ridurre il rischio per la sicurezza eliminando i potenziali vettori di attacco e riducendo la superficie di attacco del sistema stesso. A tale scopo, con un livello maggiore di dettaglio, si riportano alcune buone pratiche di hardening nell'ottica di sicurezza, specifiche dei sistemi GNU/Linux. Nel descrivere tali pratiche, ci si avvale di un indice di obbligatorietà implementativa o livello di priorità della specifica, che è necessario considerare al fine di garantire il giusto livello di sicurezza. Tale livello di priorità può assumere i seguenti valori in relazione alle relative specifiche:

- BASSO - indica che la specifica ha una priorità bassa,

- MEDIO - indica che la specifica ha una priorità media. Anche se non obbligatoria, è comunque opportuno prenderla in considerazione.
- ALTO - indica che la specifica ha una priorità alta e come tale è necessario seguire l'indicazione fornita nella specifica e implementare/apportare le modifiche consigliate.

PARTIZIONAMENTO	
Separazione delle partizioni	
Specifica	**Livello di priorità**
Garantire che "*/tmp*" e "*/var/tmp*" siano collocate su partizioni separate.	ALTO
Garantire che "*/var/log*" e "*/var/log/audit*" siano collocate su partizioni separate.	ALTO
Garantire che "*/var*" sia collocata su una partizione separata.	MEDIO
Garantire che "*/usr*" sia collocata su una partizione separata.	BASSO
Garantire che "*/home*" sia collocata su una partizione separata.	BASSO
Garantire che "*/boot*" sia collocata su una partizione separata.	BASSO
Uso delle opzioni di limitazione nei mount (/etc/fstab)	
Specifica	**Livello di priorità**
Limitare la partizione di mount "*/dev/shm*" nel seguente modo: *tmpfs /dev/shm tmpfs rw,nodev,nosuid,noexec,size=1024M,mode=1777 0 0*	MEDIO
Limitare la partizioni di mount "*/var*" e "*/var/tmp*" nel seguente modo: *mv /var/tmp /var/tmp.old* *ln -s /tmp /var/tmp* *cp -prf /var/tmp.old/* /tmp && rm -fr /var/tmp.old* *UUID=<...> /tmp ext4 defaults,nodev,nosuid,noexec 0 2*	MEDIO
Limitare la partizione di mount "*/home*" nel seguente modo: *UUID=<...> /home ext4 defaults,nodev,nosuid 0 2*	MEDIO
Limitare la partizione di mount "*/boot*" nel seguente modo: *LABEL=/boot /boot ext2 defaults,nodev,nosuid,noexec,ro 1 2*	MEDIO
Limitare la partizione di mount "*/proc*" nel seguente modo: *proc /proc proc defaults,hidepid=2 0 0*	BASSO
Limitare la partizioni di mount "*/var/log*" e "*/var/log/audit*" nel seguente modo: *UUID=<...> /var/log ext4 defaults,nosuid,noexec,nodev 0 2* *UUID=<...> /var/log/audit ext4 defaults,nosuid,noexec,nodev 0 2*	BASSO
Limitare la partizione di mount "*/var*" nel seguente modo: *UUID=<...> /var ext4 defaults,nosuid 0 2*	BASSO
Limitare la partizione di mount "*/usr*" nel seguente modo: *UUID=<...> /usr ext4 defaults,nodev,ro 0 2*	BASSO
Condivisione della memoria	
Specifica	**Livello di priorità**
Impostare il gruppo per "*/dev/shm*" come segue: *tmpfs /dev/shm tmpfs rw,nodev,nosuid,noexec,size=1024M,mode=1770,uid=root,gid=shm 0 0*	BASSO
Cifratura delle partizioni	
Specifica	**Livello di priorità**
Cifrare la partizione di "*swap*" come segue: *# Impostare in /etc/crypttab:* *sdb1_crypt /dev/sdb1 /dev/urandom cipher=aes-xts-plain64,size=256,swap,discard* *# Impostare in /etc/fstab:* */dev/mapper/sdb1_crypt none swap sw 0 0*	BASSO

ACCESSO FISICO	
Specifica di una password per il "Single User Mode"	
Specifica	**Livello di priorità**
Proteggere il "*Single User Mode*" con la password di root, come di seguito mostrato: *# Impostare in /etc/sysconfig/init.* *SINGLE=/sbin/sulogin*	BASSO
BOOTLOADER	
Protezione dei file di configurazione del "bootloader"	
Specifica	**Livello di priorità**
Assicurarsi che i file di configurazione del bootloader siano impostati correttamente. Segue un esempio: *# Impostare l'owner e group di /etc/grub.conf con quelli dell'utente root:* *chown root:root /etc/grub.conf* *chown -R root:root /etc/grub.d* *# Impostare i permessi sui file /etc/grub.conf o /etc/grub.d in modo tale che solo root può leggere e scrivere:* *chmod og-rwx /etc/grub.conf* *chmod -R og-rwx /etc/grub.d*	BASSO
KERNEL LINUX	
Log del kernel	
Specifica	**Livello di priorità**
Limitare l'accesso ai logs del kernel nel seguente modo: *echo "kernel.dmesg_restrict = 1" > /etc/sysctl.d/50-dmesg-restrict.conf*	BASSO
Kernel pointers	
Specifica	**Livello di priorità**
Limitare l'accesso ai "*kernel pointers*" nel seguente modo: *echo "kernel.kptr_restrict = 1" > /etc/sysctl.d/50-kptr-restrict.conf*	BASSO
Exec Shield	
Specifica	**Livello di priorità**
Proteggere "Exec Shield" come segue: *echo "kernel.exec-shield = 2" > /etc/sysctl.d/50-exec-shield.conf*	BASSO
Protezione della memoria	
Specifica	**Livello di priorità**
Randomizzare lo spazio di memoria nel seguente modo: *echo "kernel.randomize_va_space=2" > /etc/sysctl.d/50-rand-va-space.conf*	BASSO
LOGGING	
Syslog	
Specifica	**Livello di priorità**
Assicurarsi che il servizio *syslog* sia abilitato ed in esecuzione. A tal fine, procedere come segue: *systemctl enable rsyslog* *systemctl start rsyslog*	MEDIO
Inviare i dati *syslog* a un server esterno. Ad esempio: *# ELK* *# Logstash* *# Splunk* *# ...*	MEDIO
UTENTI E GRUPPI	
Password	
Specifica	**Livello di priorità**

Aggiornare la "*password policy*" (PAM) utilizzando il comando che segue: *authconfig --passalgo=sha512 * *--passminlen=14 * *--passminclass=4 * *--passmaxrepeat=2 * *--passmaxclassrepeat=2 * *--enablereqlower * *--enablerequpper * *--enablereqdigit * *--enablereqother * *--update*	MEDIO
Limitare il riuso delle password (PAM) nel seguente modo: *# Modificare /etc/pam.d/system-auth* *# Nel caso di pam_unix.so impostare:* *password sufficient pam_unix.so ... remember=5* *# nel caso di pam_pwhistory.so impostare:* *password requisite pam_pwhistory.so ... remember=5*	MEDIO
Rafforzare le impostazioni relative alla politica sulle password presenti nel file "*/etc/login.defs*". Procedere come segue: *# Impostare in /etc/login.defs* *PASS_MIN_LEN 14* *PASS_MIN_DAYS 1* *PASS_MAX_DAYS 90* *PASS_WARN_AGE 14*	MEDIO
Logon Access	
Specifica	**Livello di priorità**
Bloccare gli account dopo un certo numero di tentativi di accesso falliti (PAM). A tal fine procedere come segue: *# Modificare /etc/pam.d/system-auth e /etc/pam.d/password-auth* *# Aggiungere la seguente linea immediatamente prima dello statement pam_unix.so presente nella sezione AUTH:* *auth required pam_faillock.so preauth silent deny=3 unlock_time=never fail_interval=1800* *# Aggiungere la seguente linea immediatamente dopo lo statement pam_unix.so presente nella sezione AUTH:* *auth [default=die] pam_faillock.so authfail deny=3 unlock_time=never fail_interval=1800* *# Aggiungere la seguente linea immediatamente prima lo statement pam_unix.so presente nella sezione ACCOUNT:* *account required pam_faillock.so*	MEDIO
Impostare l'auto logout per inattività dell'utente. Procedere nel seguente modo: *echo "readonly TMOUT=900" >> /etc/profile.d/idle-users.sh* *echo "readonly HISTFILE" >> /etc/profile.d/idle-users.sh* *chmod +x /etc/profile.d/idle-users.sh*	BASSO
Impostare la notifica per l'ultima operazione di logon/accesso. Procedere nel seguente modo: *# Impostare in /etc/pam.d/system-auth* *session required pam_lastlog.so showfailed*	BASSO
FILESYSTEM	
Hardlinks e Symlinks	
Specifica	**Livello di priorità**
Abilitare la protezione per gli hard/soft link nel seguente modo: *echo "fs.protected_hardlinks = 1" > /etc/sysctl.d/50-fs-hardening.conf* *echo "fs.protected_symlinks = 1" >> /etc/sysctl.d/50-fs-hardening.conf*	BASSO

Mount e Unmount dinamico	
Specifica	**Livello di priorità**
Disattivare i file system non di uso comune, come segue: *echo "install cramfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install freevxfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install jffs2 /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install hfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install hfsplus /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install squashfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install udf /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install fat /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install vfat /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install nfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install nfsv3 /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install gfs2 /bin/false" > /etc/modprobe.d/uncommon-fs.conf*	MEDIO
SELINUX E AUDITD	
Utilizzo di SELinux in modalità "Enforcing"	
Specifica	**Livello di priorità**
Impostare SELinux in modalità "*Enforcing*" nel modo che segue: *# Impostare in /etc/selinux/config.* *SELINUXTYPE=enforcing*	ALTO
RETE	
TCP/SYN	
Specifica	**Livello di priorità**
Abilitare la protezione dei cookie TCP/SYN nel modo che segue: *echo "net.ipv4.tcp_syncookies = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Routing	
Specifica	**Livello di priorità**
Disabilitare il routing dell'IP sorgente nel modo che segue: *echo "net.ipv4.conf.all.accept_source_route = 0" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Protocollo ICMP	
Specifica	**Livello di priorità**
Disattivare l'accettazione del re-indirizzamento nel protocollo ICMP. A tal fine, procedere come segue: *echo "net.ipv4.conf.all.accept_redirects = 0" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Consentire di ignorare le richieste ICMP. A tal fine procedere come segue: *echo "net.ipv4.icmp_echo_ignore_all = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Broadcast	
Specifica	**Livello di priorità**
Consentire di ignorare le richieste in broadcast. A tal fine procedere come segue: *echo "net.ipv4.icmp_echo_ignore_broadcasts = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO

Seguono alcuni riferimenti utili per la Policy Compliance e la protezione delle informazioni:

- Center of Internet Security (CIS) - CIS Bemchmarks (https://www.cisecurity.org/cis-benchmarks/) - Il Center for Internet Security (CIS) è un'organizzazione senza scopo di lucro. La sua missione è di "identificare, sviluppare, convalidare, promuovere e sostenere soluzioni di best practice per la difesa informatica".
- Security Technical Implementation Guide (STIG) - Stigviewer (https://www.stigviewer.com/stigs) - Le Security Technical Implementation Guides (STIGs) sono gli standard di configurazione creati dalla Defense Information Systems Agency (DISA) per i sistemi del Dipartimento della Difesa Statunitense. Le STIG contengono una guida tecnica

per proteggere informazioni, sistemi e software, che altrimenti potrebbero essere vulnerabili a attacchi informatici dannosi in termini di diniego.

- National Institute of Standards and Technology (NIST) - National Checklist Program (NCP) (https://nvd.nist.gov/ncp/repository) - trattasi di un documento contenente istruzioni o procedure di configurazione di un prodotto informatico (IT) in un ambiente operativo, utili a verificare la corretta configurazione del prodotto stesso e/o a identificare eventuali modifiche non autorizzate a quest'ultimo.
- Payment Card Industry Data Security Standard (PCI-DSS) (https://www.pcisecuritystandards.org/pci_security/) - Il Payment Card Industry Data Security Standard (PCI DSS) è uno standard di sicurezza informatica per le organizzazioni che gestiscono carte di credito. Tale standard è stato creato per aumentare i controlli sui dati dei titolari delle carte di credito al fine di ridurne le frodi.
- Security Content Automation Protocol (SCAP) - Il Security Content Automation Protocol (SCAP) è una metodologia per l'utilizzo di specifici standard che consentono la gestione automatizzata delle vulnerabilità, la misurazione e la valutazione della conformità alle policy dei sistemi presenti in un'organizzazione, ivi inclusa, ad esempio, la conformità FISMA. Il National Vulnerability Database (NVD) rappresenta il content repository del governo statunitense per lo SCAP. Un esempio di implementazione dello SCAP è OpenSCAP.
  - SCAP Security Policies (https://www.open-scap.org/security-policies/) - insieme di regole interpretabili da una macchina a cui l'infrastruttura deve conformarsi.
  - OpenSCAP Base (https://www.open-scap.org/tools/openscap-base/) - Il tool di scansione OpenSCAP è uno strumento capace di scansionare il sistema, convalidare i contenuti di conformità alla sicurezza e generare report e indicazioni basate su tali scansioni.
  - SCAP Workbench (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sect-using_scap_workbench) - SCAP Workbench è un'utilità che consente di eseguire facilmente le comuni operazioni oscap su sistemi locali o remoti.
  - OpenSCAP Static (https://static.open-scap.org/) – documentazione OpenSCAP suddivisa in tre distinte sezioni: "API Documentation", User Manuals" e "SCAP Security Guides".
- DevSec Hardening Framework (https://dev-sec.io/) - Il progetto tratta alcuni aspetti di hardening che possono essere automatizzati (ad esempio l'impostazione della password di grub o il rafforzamento dei permessi delle directory di uso comune).

Alle linee guida generali riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Linux, le indicazioni seguenti:

BIOS Protection	
Minaccia	Possibilità di cambiare o sovrascrivere le caratteristiche di sicurezza del BIOS.
Contromisure	- È necessario proteggere il BIOS dell'host con una password in modo che l'utente finale non sia in grado di modificare e sovrascrivere le impostazioni di sicurezza nel BIOS; è importante mantenere quest'area protetta da eventuali modifiche. Ogni produttore di computer ha un set diverso di modalità di accesso al BIOS che dovrebbe essere comunque protetto utilizzando queste modalità. Proteggere GRUB con password per limitare l'accesso fisico al sistema. - Inoltre, è necessario disabilitare l'avvio da dispositivi multimediali esterni (USB / CD / DVD). Se si omette di modificare questa impostazione, chiunque può utilizzare una chiavetta USB che contenga un sistema operativo avviabile e accedere ai dati del sistema operativo. - I server linux più recenti dispongono di applicazioni Web attraverso le quali è

	possibile, accedendo da remoto, configurare le caratteristiche di sistema. Bisogna assicurarsi di cambiare la password predefinita o, eventualmente, disattivare questa possibilità.

Hard disk encryption	
Minaccia	Possibilità di accedere, ad esempio, tramite boot da sistema operativo esterno ai dati presenti sui dischi della macchina linux.
Contromisure	La maggior parte delle distribuzioni Linux consentono di crittografare i dischi prima dell'installazione o successivamente tramite software opportuni. La crittografia del disco è importante in caso di furto o di accesso fraudolento perché il malintenzionato non sarà in grado di leggere le informazioni presenti sui dischi stessi anche collegando il disco rigido ad un altro computer.

Lock boot directory	
Minaccia	La "boot directory" contiene file importantissimi relativi al kernel Linux, quindi è necessario assicurarsi che questa directory sia bloccata con autorizzazioni di sola lettura.
Contromisure	Il lock della boot directory va eseguito seguendo alcuni semplici passaggi. Aprire con un editor il file “fstab” (path usuale /etc/fstab) e aggiungere la riga LABEL=/boot /boot ext2 defaults 1 2 (i valori di riferimento ext2 possono variare a seconda della configurazione del sistema linux). Al termine della modifica del file, è necessario impostare il proprietario eseguendo il seguente comando: #chown root:root /etc/fstab Successivamente, vanno impostate alcune autorizzazioni per la protezione delle impostazioni di avvio: Come già indicato nelle pratiche precedentemente descritte, impostare il proprietario e il gruppo di /etc/grub.conf all'utente root: #chown root: root /etc/grub.conf Impostare il permesso sul file /etc/grub.conf per leggere e scrivere solo per root: #chmod og-rwx /etc/grub.conf Richiedere l'autenticazione per la modalità "single user": #sed -i "/ SINGLE / s / sushell / sulogin /" / etc / sysconfig / init #sed -i "/ PROMPT / s / yes / no /" / etc / sysconfig / init

Disabilitare l'utilizzo di device USB	
Minaccia	Attraverso l'uso di device USB un utente malintenzionato potrebbe accedere al sistema linux come utente amministratore oppure potrebbe accedere a informazioni o dati sensibili del sistema stesso.
Contromisure	A seconda della criticità del sistema, a volte è necessario disabilitare l'uso delle chiavette USB sull'host Linux. Esistono diversi modi per bloccare l'utilizzo di un device USB. Di seguito viene descritto uno dei metodi principali: - Aprire con un editor e modificare il file “blacklist.conf” (path usuale /etc/modprobe.d/blacklist.conf) come indicato. - Aggiungere alla fine del file la riga: - blacklist usb_storage - Salvare e chiudere il file blacklist.conf. - Aprire con un editor e modificare il file rc.local (path usuale /etc/rc.local) - Aggiungere alla fine del file le due righe seguenti: - modprobe -r usb_storage

	- exit 0 - Salvare e chiudere il file rc.local. Eseguire la ripartenza della macchina per rendere effettive le modifiche.

Aggiornamenti di Sistema	
Minaccia	Avere un Sistema non aggiornato può rendere vulnerabile la macchina da attacchi di utenti malintenzionati.
Contromisure	La prima cosa da fare dopo il primo avvio è aggiornare il sistema operativo. La procedura in genere non è complessa e può essere fatta sia da una finestra terminale che per la maggior parte dei sistemi linux anche tramite tool grafici di amministrazione del sistema.

Controllo dei pacchetti installati	
Minaccia	La presenza di servizi non necessari può rappresentare un rischio per la sicurezza del sistema.
Contromisure	Successivamente all'installazione del sistema operativo deve essere effettuato dagli amministratori della macchina un elenco di tutti i pacchetti installati sul SO Linux. Vanno quindi rimossi tutti i pacchetti non necessari. La selezione deve essere molto approfondita per le macchine con tipologia di server perché i server hanno bisogno di un minor numero di applicazioni e servizi installati. Nel caso di server Linux, in particolare, è importante rimuovere i seguenti servizi perché non necessari per il normale utilizzo di un server linux: - Telnet server - RSH server - NIS server TFTP server TALK server

Secure Shell (SSH)	
Minaccia	Secure Shell (SSH) è un protocollo utilizzato per fornire comunicazioni sicure e crittografate su una rete. È più utilizzato dagli amministratori di sistema Linux per la gestione remota dei server. Può anche essere utilizzato per trasferire file su una rete. Per queste caratteristiche la sicurezza SSH è molto importante.
Contromisure	Il protocollo SSH, pur essendo abbastanza sicuro, necessita di una corretta e approfondita configurazione per poter essere utilizzato senza rischi. A tal fine vanno eseguiti tutta una serie di passi sul file file di configurazione "sshd_config" (path usuale /etc/ssh). Tra i principali settaggi di seguito ne verranno elencati i principali: - Cambio delle porte di default del servizio SSH - Configurare SSH per autenticarsi tramite delle chiavi SSH invece di password - Usare il protocollo SSH2 invece di SSH1 - Usare una lista predefinita di possibili accessi di utenti ("User Whitelist") o in alternativa usare delle "Blacklist" di utenti bloccati. - Disabilitare l'accesso tramite root login Se non strettamente necessario è possibile anche eliminare la possibilità di accesso tramite SSH.

Controllo delle porte aperte su linux

Minaccia	La gestione delle porte aperte su linux ed in particolare delle connessioni Internet aperte è fondamentale su linux ai fini della sicurezza del sistema in merito a possibili attacchi di malintenzionati.
Contromisure	Vanno verificate tutte le porte aperte con attenzione particolare a porte nascoste. Su molte versioni di linux, ad esempio, è possibile individuare eventuali porte aperte nascoste tramite il comando: `#netstat –antp` Dopo aver configurato i servizi della rete, è quindi molto importante sapere quali porte sono in ascolto sulle interfacce di rete del sistema. Qualsiasi porta aperta può essere segno di una intrusione. Sono presenti due approcci di base per poter elencare le porte in ascolto sulla rete. L'approccio meno affidabile è quello di interrogare lo stack della rete, inserendo dei comandi del tipo `netstat –an o lsof –i`. Questo metodo è meno affidabile in quanto questi programmi non si collegano alla macchina dalla rete, ma cercano di sapere cosa viene eseguito sul sistema. Per questa ragione, queste applicazioni sono bersaglio da parte di aggressori. In questo modo, i cracker cercano di coprire le loro tracce nel caso in cui essi aprono delle porte di una rete non autorizzata. Il modo più affidabile di controllare quali sono le porte in ascolto sulla rete, è quello di usare uno scanner del tipo nmap. Il seguente comando emesso dalla console, determina quali sono le porte in ascolto dalla rete per collegamenti TCP: `nmap –sT –O localhost`

Password policies	
Minaccia	Una gestione non corretta nella gestione delle "Password policies" aziendali può rappresentare una possibile falla nella sicurezza del sistema.
Contromisure	Una possibile fonte di criticità nella sicurezza nei sistemi operativi è rappresentata dal fatto che le persone spesso riutilizzano le loro password, consuetudine che rappresenta una cattiva pratica di sicurezza. Questa modalità può essere controllata e ed eventualmente impedita tramite interventi sui file di configurazione di sistema. Un'altra politica sulle password che dovrebbe essere forzata è obbligare ad usare solo password con certi regole. Esistono moduli o utility che proteggono il server tramite l'uso di dizionari e metodologie contro attacchi di tipo brute-force. Sarebbe opportuno anche assicurarsi di definire un algoritmo di hashing della password sicuro ad esempio di tipo SHA512. Un'altra funzionalità interessante è bloccare l'account dopo cinque tentativi falliti. Inoltre, un'altra buona pratica è impostare la scadenza della password dopo 90 giorni. Queste attività possono essere eseguite in varie modalità sui sistemi linux. Per esempio: settare il parametro PASS_MAX_DAYS a 90 nel file "/etc/login.defs". E' possibile anche modificare dinamicamente il parametro con il comando linux: #change --maxdays 90 <user>

Partizionamento	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi.
Contromisure	Come precedentemente illustrato nelle pratiche di sicurezza, in fase di installazione del sistema Linux, è necessario creare delle partizioni distinte per i seguenti percorsi: - / - /boot

	- /home - /tmp - /var/log - /var/log/audit Queste partizioni devono essere utilizzate nel seguente modo: - Sulla partizione di boot devono esser salvati tutti i file necessari ad un corretto avvio del sistema - Sulla partizione /tmp devono esser salvati tutti i file temporanei necessari al corretto funzionamento del sistema e il path /var/tmp dovrà esser collegato, tramite link e irreversibilmente, alla partizione /tmp - Sulla partizione /home devono esser salvati tutti i dati relativi alle utenze presenti sul sistema e ai loro ambienti - Sulle partizioni /var/log* devono esser salvati tutti i file di log e auditing Altri applicativi particolarmente esigenti in termini di spazio e non inclusi nella distribuzione Linux, devono essere installati in partizioni separate (es. Oracle, DB2, ecc.). L'utilizzo di diverse partizioni permette di salvaguardare l'integrità e la riservatezza dei file di configurazione, dei file di log e dei dati applicativi.

Opzioni di mount delle partizioni	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Errori di amministrazione dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Specificare le seguenti opzioni di mounting per la partizione /tmp: - nodev - nosuid - noexec - strictatime (visualizzato come relatime dall'output comando "mount") Specificare la seguente opzione di mounting per la partizione /home: - nodev Non devono esser utilizzate periferiche esterne removibili. Nel caso se ne renda necessario l'utilizzo, specificare le seguenti opzioni di mounting in /etc/fstab: - nodev - nosuid - noexec Utilizzare le seguenti opzioni di mounting per il path relativo alla memoria condivisa: - nodev - nosuid - noexec L'utilizzo di questi parametri evita l'esecuzione di file malevoli e l'escalation dei privilegi sul server, o l'accesso non autorizzato a periferiche di sistema.

Cartelle scrivibili da chiunque	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Sul sistema non dovrebbero esistere cartelle scrivibili da chiunque, modificare, per tali cartelle, i permessi di scrittura per OTHER in modo più restrittivo. Nel caso in cui tale configurazione dei diritti di accesso sia strettamente necessaria, configurare i permessi di tutte le cartelle riscrivibili da tutti per far sì che nessun utente possa cancellare e modificare i file di cui non è proprietario. Impostare di conseguenza lo "sticky bit", su tutte le cartelle riscrivibili da tutti.

UMASK	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Configurare la umask di default sia per root sia per gli altri utenti in modo che: - Ogni nuovo file creato possa essere modificato o cancellato esclusivamente dal suo owner - Ogni nuovo file creato possa esser acceduto solo da parte degli utenti appartenenti al gruppo dell'owner stesso Questa configurazione permette di avere un controllo nativo sulla riservatezza e sull'integrità di tutti i nuovi file.

Single User Mode e Boot Interattivo	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Danneggiamento, perdita o furto di un asset fisico.
Contromisure	Abilitare il controllo di autenticazione per l'accesso alla modalità single-user al fine di impedire la compromissione del sistema da parte di utenti non autorizzati in grado di accedere fisicamente alla console del sistema. Disabilitare il boot interattivo per gli utenti di sistema (tasto I al boot) al fine di

	contrastare l'utilizzo improprio di comandi sistemistici in fase di avvio del sistema operativo.

Sicurezza TCP/IP	
Minaccia	- Negazione dei servizi. - Compromissione delle comunicazioni.
Contromisure	È necessario mettere in sicurezza lo stack TCP/IP attraverso le seguenti impostazioni: - Disabilitare l'IP forwarding al fine di impedire che il server in esame funga come base di attacco verso ulteriori sistemi nella rete. - Disabilitare l'invio e l'accettazione di pacchetti ICMP Redirect. - Disabilitare l'accettazione di pacchetti ICMP Redirect anche se questi provengono da gateway trusted (ICMP Secure Redirect). - Disabilitare i pacchetti "source routed". - Abilitare i log per i pacchetti di rete ricevuti, aventi un indirizzo di origine non-routable (privo di una rotta in tabella di routing). - Ignorare i pacchetti ICMP Echo inviati in broadcast. - Disabilitare il logging nel caso di ricezione di pacchetti broadcast non conformi allo standard RFC-1122 al fine di impedire la saturazione dello spazio destinato ai file di log. - Abilitare il "reverse path filtering". - Abilitare i "SYN cookies" per la gestione dell'handshake TCP SYN/ACK. - Disabilitare l'IPv6 (se non utilizzato) in modo da ridurre la superficie di attacco del sistema.

Utenti e gruppi di default	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Disabilitare le utenze di default non utilizzate ma definite sul sistema quali: - lp - news - uucp - games - gopher - ftp - vcsa - rpc - smmsp - pcap - desktop Disabilitare i gruppi di default non utilizzati quali: - lp - news - uucp - games

PATH di root	
Minaccia	- Attacchi all'integrità dei sistemi. - Errori di amministrazione dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).

Contromisure	L'utenza root deve avere la variabile di ambiente PATH definita con i soli percorsi necessari all'esecuzione delle operazioni di default. Definire, ad esempio, PATH="/usr/bin:/usr/sbin:/sbin" e non inserire in alcun caso il path "." . Nel caso in cui siano presenti specifiche directory, diverse da quelle standard, per esigenze particolari, tali directory devono risultare scrivibili solo da root ed eventualmente dall'utente proprietario, se diverso da root.

Accessi amministrativi impersonali	
Minaccia	- Violazione di leggi, di regolamenti, di obblighi contrattuali. - Uso non autorizzato di privilegi. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Disabilitare il login remoto per l'utenza amministrativa root e per altre utenze impersonali (es. "oracle", ecc.), al fine di assicurare il corretto tracciamento delle attività svolte dagli amministratori di sistema e la corretta associazione tra le attività svolte e le persone fisiche che le hanno effettivamente attuate. Gli amministratori di sistema dovranno accedere con utenze personali univoche e successivamente utilizzare il comando "sudo" per effettuare operazioni privilegiate. Le utenze personali possono essere definite sul sistema, o per maggiore praticità il sistema può essere integrato con un server di autenticazione centralizzato basato su LDAP o Active Directory, ad es. tramite moduli PAM.

Tentativi di accesso ripetuti	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Impostare un limite per i tentativi di accesso remoto al sistema (3 tentativi) e un blocco temporaneo (generalmente 30 minuti) al raggiungimento di tale limite.

Minimizzazione dei servizi	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Disabilitare tutti i servizi non necessari, al fine di ridurre i vettori di attacco al sistema e il numero di vulnerabilità associate a servizi non necessari e insicuri. In particolare. Disabilitare X-Windows se non necessario, e tutti i servizi legacy basati su inetd e non utilizzati, ovvero chargen, daytime, discard, echo, time, tftp. Disabilitare inoltre I seguenti servizi autonomi: - avahi-daemon - cups (server di stampa) - dhcpd (server DHCP) - slapd (server LDAP) - nfs - rpcbind - named (server DNS)