› If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

› If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

› If the evaluated student chose Debian: the difference between aptitude and apt, and what APPArmor is. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

link git-hub con subject e domande per correzione

link del subject usato per rispondere alle domande:
(ci sono le risposte gia messe nel subject)

https://github.com/gemartin99/Born2beroot-Tutorial/blob/main/README_EN.md#9--correction-sheet-

---

> SIGNATURE.TXT <

//
NON APRIRE LA MACCHINA DOPO AVER CONSEGNATO, CIO' CAMBIERA' LA SIGNATURE DELLA MACCHINA
//

-shasum Born2beroot.vdi (da terminale (ovviamente prima spostarsi nella cartella in cui e' l amacchina))
permette di vedere la signature della macchine, il processo e' lento quindi non spaventarti se ci mette un po'

> PROJECT OVERVIEW <

---

how a virtual machine works -->

Una macchina virtuale (VM) è un software che emula un computer fisico e permette di eseguire un sistema operativo (SO) e applicazioni come se fossero su un hardware dedicato. Il funzionamento di una VM si basa sulla virtualizzazione, una tecnologia che separa il software dal sottostante hardware fisico.

---

choice of the operating system -->

sono due formati di linux che differiscono nell'adattamento delle loro funzionalità, debian è più accessibile e semplice da usare per l'utente medio
mentre rocky è adattato alle esigenze delle aziende
(da arogomentare meglio se possibile)
DISTRIBUZIONE: Debian e open source e gestito da volontari:
Rocky e gestita da Rocky Enterprise Software Foundation.

STORIA: Debian nasce nel 1993 da un gruppo di utenti volontari:
la filosofia di Debian emerge dal Debian social contract,

che rappresenta l'etica dietro al progetto:
- Debian rimarrà libera al 100%
- Renderemo [un prodotto valido] alla Comunità Free Software
- Non nasconderemo i problemi
- Le nostre priorità sono gli utenti ed il software libero

Rocky nasce nel 2020, come una evoluzione di CentOs, una distribuzione Linux che ha smesso di ricevere supporti dalla propria azienda (Red hat).

COMPATIBILITA: Debian, grazie alla sua architettura minimalista, e compatibile con qualsiasi hardware;
Rocky e progettato per essere performante con gli hardware piu recenti.

/\
|
the differences

---

the purpose of the virtual machine -->

lo scopo delle virtual machine e quello di avere un altro sistema operativo all'interno del pc al fine di creare un ambiente in cui è possibile isolare l'intero computer da potenziali minacce

(oppure avere un ambiente di lavoro univico per l'azienda e in maniera che sia tutto gia preparato per l'utilizzo)

---

if the student chose rocky what is DNF and SELinux -->

non si vuole fare perche non ci serve pero si lascia
https://youtu.be/kw1kc2U6NmA?si=NJ3_XWvZYmO98EKq

---

if the student chose Debian what is the difference between apt and aptitude, and what is APPArmor?
(during the defence the script must display information all every 10 minuts)
-->

-apt :
apt strumento per la gestione dei pacchetti su sistemi operativi basati su Debian (come Ubuntu). Servono per installare, aggiornare e rimuovere software. APT e' un low-level package

-aptitude :
ti offre una interfaccia (che non si deve usare) per fare
la stessa cosa di apt. Aptitude e' un high-level package. Piu' ricco di features, piu' "intelligente" ma meno veloce.

-appArmor :

AppArmor (Application Armor) è un sistema di sicurezza basato su MAC (Mandatory Access Control) per i sistemi Linux.
A cosa serve:
Protegge il sistema controllando a quali risorse (file, rete, memoria) le applicazioni possono accedere.
Applica regole specifiche a ogni applicazione per limitarne l'accesso.

Funzionamento:
Usa profili predefiniti o personalizzati per applicare restrizioni.
Ad esempio, un profilo può permettere a un'applicazione di leggere determinati file, ma impedirle di scrivere in essi.

LVM: e un metodo di gestione dello spazio di memoria.
Di norma, lo spazio sul disco puo essere diviso in sottospazi di memoria.
Questi sottoinsiemi si dividono in partizioni primarie e logiche.
Le partizioni primarie possono essere massimo 4: una volta create, non e piu possibile creare altre sottopartizioni.
Una delle partizioni primarie puo essere una partizione estesa, e puo avere la possibilita di contenere altre partizioni: le partizioni logiche.
Una partizione estesa NON puo contenere dati che non siano partizioni logiche.
Una partizione logica e quindi un'area allocata in una partizione estesa.
PROBLEMA: questo metodo e molto rigido: espandere la memoria di una partizione fa si che "invada" le altre aree di memoria: se due partizioni sono adiacenti in memoria, aggiungere memoria ad una implica muovere l'altra.
inoltre, fare modifiche implica modificare fisicamente lo spazio sul disco, e percio e necessario riavviare il sistema per rendere effettiva ogni modifica.

LVM (Logical Volume Manager) risolve questi limiti: unendo piu volumi fisici (physical volumes), composti da dischi e partizioni primarie, crea una unica area di memoria (volume groups), all'interno della quale crea a sua volta delle partizioni logiche.
Offre un vasto ventaglio di funzionalita all'utente:
- Ridimensionamento dinamico: come detto, permette di aumentare o ridurre la dimensione di un volume logico senza ridimensionare fisicamente lo spazio fisico (la partizione primaria);
- Snapshot: permette di creare istantanee di un volume in un dato momento. E quindi possibile fare backup sulla memoria;
- Aggregazione di spazio: aggrega piu dischi e partizioni logiche in una unica area;
- Spostare dati: permette di spostare dati tra dischi diversi senza downtime (= riavvio del sistema).

LVM ha anche degli svantaggi:

- usare LVM e piu lento rispetto alla gestione diretta delle partizioni
fisiche;
- se non configurato direttamente, c'e il rischio di corruzione dati.

> SIMPLE SETUP <

---
ensure that the machine as no graphic and put the password to login -->

-si puo' verificare visivamente, che non abbia interfaccia grafica, o si puo' usare il comando ls /usr/bin/*session

-sudo adduser "username":
aggiunge un utente

-sudo addgroup "evaluationgroup"
crea un gruppo chiamato evaluation group

-sudo adduser "username" "evaluationgroup"
per aggiungere il nuovo utente all'interno del nuovo gruppo

-getent group "groupname"
mostra gli utenti all'interno del gruppo che si vuole prendere in considerazione

---
check UFW(e il firewall) -->

-sudo service ufw status
controlla lo stato di ufw
(Un firewall è un sistema di sicurezza progettato per monitorare, filtrare e controllare il traffico di rete in base a regole predefinite per maggiori info domade born2BeRoot)
---
check the ssh -->

-sudo service ssh status
controla se l'ssh è attivo
---
check that the operating system is debian or rocky?

-uname -v
ti fa vedere se stai utilizzando debian o rocky

> USER <

-sudo adduser "username":
aggiunge un utente

-sudo addgroup "evaluationgroup"
crea un gruppo chiamato evaluation group

-sudo adduser "username" "evaluationgroup"
per aggiungere il nuovo utente all'interno del nuovo gruppo

-getent group "groupname"
mostra gli utenti all'interno del gruppo che si vuole prendere in considerazione
---

> HOSTNAME AND PARTITION <

---
check that the hostname of the machine is correct

-hostname
printa l'hostname
---
modify the hostname of the machine

-sudo nano /etc/hostname
ti apre il file system con l'hostname in cosi' puoi cambiarlo

-sudo nano /etc/hosts
ti apre il file system nel quale devi modificare il login con il nuovo login

-sudo reboot
---
how to view the partition

-lsblk
mostra le partizioni

> SUDO <

---
check that sudo program is properly installed

-dpkg -s sudo
ti mostra che sudo e' stato installato correttamente
dpkg = Debian Package
---
add the new user to the sudo group

-sudo adduser "username" sudo
aggiunge al gruppo sudo il nuovo utente
---
show and explain the rules for sudo

-nano /etc/sudoers.d/sudo_config
mostra le regole che abbiamo implementato per sudo
---
show that the path /var/log/sudo/ exists and contains at least one file, in this we should see a history of the commands used with sudo

-cd /var/log/sudo
per muoversi

-ls
mostra i file all'interno della directory

-cat sudo_config
printa il contenuto del file sudo_config, che sarebbe la cronologia dei comandi
---

> UFW <

---
check if the UFW program is properly installed and that it worked correctly

-dpkg -s ufw
ti fa vedere che ufw e' stato installato correttamente

-sudo service ufw status
ti fa vedere che ufw e' abilitato e funziona correttamente
---
list the active rule for UFW

-sudo ufw status numbered
---
create a new rule for port 8080. Verify that it has been added to the active rules and then you can delete it

-sudo ufw allow 8080
per creare la regola

-sudo ufw status numbered
ti mostra che la regola sia stata creata correttamente

-sudo ufw delete "numero della regola (da controllare col comando precedente)"
cancella la regola

> SSH <

---
check that the ssh service is properly installed and that it work correctly

-which ssh

-sudo service ssh status
---
verify that the ssh service only uses port 4242

-sudo service ssh status
---
use ssh to log in the machine from the terminal and make sure that you can't log with the root

-(in terminal)ssh "username"@"ip address" -p 4242
serve per collegrti alla macchina virtuale

> SCRIP MONITORING <

---
modify the runtime of the script from 10 to 1 minute

-sudo crontab -u root -e
ti apre il file da modificare, modifica il primo numero con 1 al posto di 10
---
make the crontab stop running

-sudo /etc/init.d/cron stop || -sudo systemct1 stop cron (nel caso il primo comando non funzionasse)
per fermarlo

-sudo /etc/init.d/cron start || - sudo systemct1 strart cron (nel caso il primo comando non funzionasse)
per farlo ricominciare

-sudo service cron status
per verificare lo status della crontab