

b2b TODO-LIST

Born2beRoot Defense Checklist

By Adrian Musso-Gonzalez (@amusso-g)

https://docs.google.com/document/d/1-BwCO0udUP7MhRh81Y681zz0BalXtKFtte_FHJc6G4s/edit

該当の.utmファイルのパス

shasum Images/disk-0.qcow2

Preliminary tests

- Git repo cloned successfully.
Git リポジトリのクローンに成功しました。

General instructions

- Git repo contains a signature.txt file.
Git リポジトリには signature.txt ファイルが含まれています。
- Check the signature against the students ".vdi" file, make sure it's identical.
生徒の".vdi"ファイルと署名を照合し、同一であることを確認する。
- Clone VM || create a snapshot && open VM.
VMのクローン | スナップショットを作成し、VMを開く。

Mandatory Part (Questions for the student)

- ***How does a virtual machine work and what is its purpose?***

仮想マシンはどのように動作し、その目的は何ですか？

プログラムやアプリを実行するために、物理的なコンピュータの代わりにソフトウェアを使用するリソース。各VMは独自のオペレーティング・システムを持ち、別々に機能するため、1台のマシンに複数のVMを持つことができる。安全で独立した環境でアプリケーションをテストするために使用することができる。ソフトウェアを使って仮想ハードウェアをシミュレートし、ホストマシン上で実行することで機能する。

- **ホスト型の仮想マシン**

物理マシンにWindowsやLinuxなどのOSをインストールして、その中に仮想ソフトウェアとなるアプリケーションをインストールして、仮想マシンを実現させる方式のこと。

→既に利用しているパソコンやサーバーにも簡単にインストールできるため、導入しやすい。

- VMware Player
- Microsoft Virtual PC
- Oracle Virtual Box

- **ハイパーバイザー型の仮想マシン**

ホストのOSを使わずに直接サーバーにソフトウェアをインストールして仮想マシンを実現する方式のこと。現在、最も主流な方式としてハイパーバイザー型が浸透している。

→ホストOSが不要で直接ハードウェアを制御できるようになることから、仮想マシンの処理速度低下を最小限に抑えられる。

- VMware vSphere ESXi
- Citrix XenServer
- Hyper-V
- KVM

- **コンテナ型の仮想マシン**

物理マシンにWindowsやLinuxなどのホストOSをインストールして、コンテナ管理ソフトウェアをインストールして利用する方式。コンテナ型は、アプリケーションやソフトウェアを実行環境と共にコンテナイメージ（コンテナのテンプレートファイル）として包括することから、コンテナ型と呼ばれています。

→ コンテナイメージやソフトウェアそのものが軽量

- Docker

- *The basic differences between CentOS and Debian?*

CentOS（rocky）とDebianの基本的な違い？

Debian は、新しいバージョンがリリースされたときに、CentOS よりもずっと簡単にアップデート可能。Debian はよりユーザーフレンドリーで、多くのライブラリ、ファイルシステム、アーキテクチャーをサポートしている。また、カスタマイズのためのオプションもより多く存在。大規模なビジネスであれば、CentOS はより多くの商用機能を提供している点で優れている。

- *Their choice of operating system?*

彼らのOSの選択？

インストールや設定が簡単だから、個人サーバーに最適。

- *If Debian: the difference between aptitude, apt and what APPArmor is.*

Debianの場合：aptitudeとaptの違い、APPArmorとは何か。

	apt	apt-get	aptitude
違い	apt-getの設計上のミスを修正	設計にミスあり	APTの外部プロジェクトとして生まれたGUIをもったもの(未完成)
使用推奨	○	x	x
アップグレード方法	apt upgrade	apt-get upgrade	aptitude safe-upgrade
アップグレードのパッケージ選択規則	緩い	現在のパッケージ構成を変えないため厳しい	緩い
フルアップグレード	apt-get dist-upgrade	apt full-upgrade	aptitude dist-upgrade
自動的にインストールされたパッケージの追跡	ユーザが手作業でこのコマンドを実行するべきではないためコマンドなし	apt-get autoremoveで不要になった自動パッケージを削除	不要な自動パッケージを見つけ次第自動的に削除するためコマンドなし

Aptitude は高レベルのパッケージマネージャであり、APT は他の高レベルのパッケージマネージャで利用できる低レベルのパッケージです。

Aptitude はより賢く、使っていないパッケージを自動的に削除したり、依存するパッケージのインストールを提案したりします。

Apt はコマンドラインで指示されたことのみを明示的に実行します。

→ <https://ultra-genma.hateblo.jp/entry/2019/04/08/233718>

※AppArmorとは？

MAC (Mandatory Access Control) セキュリティを提供するLinuxセキュリティシステムです。システム管理者がプロセスが実行できるアクションを制限することを

可能にします。Debianにデフォルトで含まれています。aa-statusを実行して、実行されているかどうかを確認します。

AppArmor とは、プログラム単位でMAC(Mandatory Access Control - 強制 アクセス制御)を行うためのセキュリティ機構のこと。

MACとは、従来のファイルのパーミッションの設定等とは関係なく、強制的にアクセス制限を設けることができる。

AppArmor では、プログラム毎に、ファイルやソケットなどに対して行う ことのできる操作を明示的に指定し、それ以外の操作を行えなくすることができます。→セキュアな環境の構築が可能。

<https://www.usupi.org/sysad/220.html>

UFW

- During the defense, a script must display all information every 10 minutes. Its operation will be checked in detail later.

防御の間、スクリプトは10分ごとにすべての情報を表示しなければならない。その動作は後で詳しく確認する。

- All explanations are satisfactory (else evaluation stops here).

すべての説明は満足のいくものである（そうでなければ評価はここでストップする）。

Simple setup

- Ensure that the machine does not have a graphical environment at launch.

マシンが起動時にグラフィカルな環境でないことを確認します。

- Connect to VM as a created user (which isn't a root)

作成したユーザ（rootでない）でVMに接続する。

- Ensure the password follows the required policy (2 days min, 7, 30 days max).

パスワードが必要なポリシーに従っていることを確認 (最低2日、7日、最大30日)

sudo chage -l username

- Evaluator checks UFW service is started.

EvaluatorはUFWサービスが開始されていることを確認します。

sudo ufw status *//look for status: active*

- Evaluator checks SSH service is started.

SSHサービスが開始されていることを確認します。

sudo systemctl status ssh

- Evaluator checks the chosen operating system (Debian or CentOS).

選択したオペレーティングシステム(DebianまたはCentOS)をチェックします。

lsb_release -a || cat /etc/os-release

uname -a

User

- The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to “sudo” and “user42” groups.

評価対象者は、評価対象の学生のログイン名を持つユーザーが仮想マシンに存在することを要求します。追加されていることと、「sudo」「user42」グループに所属していることを確認してください。

cat /etc/passwd | grep rwatanab

getent group sudo

getent group user42

□ 自分のログイン名とするユーザーを作成し、`user42` と `sudo` グループに所属させる

- Create new user (e.g. user42).

新しいユーザー（例：user42）を作成します。

`new_demo`

`Born2BeRoot`

`sudo adduser new_username`

- Assign a password of your choice, respecting subject rules.

サブジェクトのルールを尊重しながら、好きなパスワードを割り当てる。

`sudo usermod -aG sudo new_demo`

`getent group sudo`

- Explanation from student explaining how to implement the password policy.

パスワードポリシーの実行方法を説明する学生からの説明。

パスワードのルールには、パスワード品質チェックライブラリを使用し、大文字と小文字、重複文字などのルールを設定するcommon-passwordファイルと、パスワードの有効期限ルール（30日など）を格納するlogin.defsファイルの2つのファイルがあります。

`sudo nano /etc/login.defs`

`sudo nano /etc/pam.d/common-password`

以下で確認！

`sudo vi /etc/pam.d/common-password`

↓ポリシーは以下を設定。

`password requisite pam_pwquality.so`

`retry=3`

minlen=10

ucredit=-1 dcredit=-1

※大文字・数字

↓-1の理由

マイナス値で指定した場合、指定した文字種が指定した値の数含まれていなければならない


https://mseeeen.msen.jp/how-to-set-password-policy-in-centos7/#_minlen

maxrepeat=3

reject_username difok=7

enforce_for_root

Debian 10 Buster : パスワードポリシーを設定する : Server World

 https://www.server-world.info/query?os=Debian_10&p=password

- ☐ 有効期限は30日
- ☐ 最短利用日数は2日
- ☐ 有効期限の7日前に警告メッセージを発する
- ☐ 10文字以上
- ☐ 大文字と数字を含む
- ☐ 小文字
- ☐ 最大連続文字数は3
- ☐ ユーザ名を含まない
- ☐ 変更前に含まれる文字が変更後のパスワードに7文字以上含まれてはならない

- Normally there should be one or two modified files. If there is any problem, the evaluation stops here.

通常、変更されるファイルは1つか2つであるはずですが、もし問題があれば、評価はここで終了します。

- With the new user, ask the student to create a group named “evaluating” and assign it to the new user.

新しいユーザで、"evalating" という名前のグループを作成し、新しいユーザに割り当てるよう学生に依頼します。

sudo groupadd evaluating

sudo usermod -aG evaluating your_new_username

- Check if the new user belongs to the “evaluating” group.

新しいユーザが "evaluating" グループに属しているかどうか確認します。

getent group evaluating

- Ask the student to explain advantages of the password policy (beyond the fact that it is required for the project)

パスワードポリシーの利点(プロジェクトに必要であるという事実以外)を説明するように学生に頼む

- Ask the student the advantages/disadvantages of the policy implementation.

ポリシー導入のメリット/デメリットを生徒に質問する。

Hostname and partitions

- **Check the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).**

マシンのホスト名が次のように正しくフォーマットされていることを確認する:
login42 (評価対象の学生のログイン)

hostnamectl

☐ ホスト名を ログイン名 + 42 にする

- Modify this hostname by replacing the login with yours, then restart VM.

ログイン名を自分のものに置き換えてこのホスト名を変更し、VMを再起動します。

`sudo hostnamectl set-hostname new_hostname`

`sudo vi /etc/hosts`

→rwatanab42部分を新しいものに変える

`sudo reboot`

Note: If on restart, the hostname has not been updated, the evaluation stops here.

Note: 再起動時にホスト名が更新されていない場合、評価はここで中断されます。

- Restore the machine to the original hostname, then restart VM.

マシンを元のホスト名に復元してから、VMを再起動します。

`sudo hostnamectl set-hostname new_hostname`

`sudo reboot`

- Ask the student being evaluated how to view the partitions for the VM.

VM のパーティションを表示する方法を評価される学生に尋ねます。

`lsblk`

- Compare the output with the example given in the subject (if there are bonuses, refer to the bonus example).

出力を課題文中の例と比較する(ボーナスがある場合は、ボーナス例を参照する)。

- Ask the student for a brief explanation of LVM and how it works.

生徒にLVMとその動作について簡単に説明するよう求める。

Logical Volume Manager –

論理ボリュームマネージャー - ストレージデバイス上のパーティションや論理ボリュームを簡単に操作することができる。

☐ 暗号化LVMを使用してpdfにあるようなパーティションを作成

SUDO

- **Check that the “sudo” program is properly installed on the virtual machine.**

“sudo”プログラムが仮想マシンに適切にインストールされていることを確認します。

dpkg -l | grep sudo

- The student being evaluated shows assigning a new user to the “sudo” group.
評価される学生は、新しいユーザを「sudo」グループに割り当てることを示しています。

- The subject imposes strict rules for sudo. The student being evaluated must explain the value and operation of sudo using examples of their choice.

対象はsudoの厳格な規則を課しています。評価される学生は、選択した例を用いてsudoの価値と操作を説明する必要があります。

sudo visudo ls

- Second step, must show the implementation of the rules imposed by the subject.

第二段階として、被験者が課したルールの実装を示す必要があります。

- Verify the “/var/log/sudo/” folder exists and has at least one file. Check the contents of the files in the folder, you should see a history of the commands used with sudo.

`/var/log/sudo/` フォルダが存在し、少なくとも 1 つのファイルがあることを確認する。フォルダ内のファイルの内容を確認し、あなたはsudoで使用されるコマンドの履歴が表示されるはずです。

入力の履歴：

`cat /var/log/sudo/sudo.log`

出力の記録：

`sudo sudoreplay /var/log/sudo/00/00/01`

- Run a command via sudo. See if the file(s) in the “`/var/log/sudo/`” folder have been updated.

sudoでコマンドを実行します。`/var/log/sudo/` フォルダ内のファイルが更新されているかどうかを確認します。

`/etc/sudoers` を直接編集してミスると大変らしいので `visudo` を使う

☐ sudo を使用した認証は、パスワードが正しくない場合、試行回数を 3 回に制限する。

☐ sudoの使用時にパスワードの間違いによるエラーが発生した場合、任意のカスタムメッセージを表示する。

☐ sudo を使用する各アクションを、入力と出力の両方をアーカイブする。ログファイルは `/var/log/sudo/` フォルダに保存。Defaults `iolog_dir="/var/log/sudo"`

☐ セキュリティ上、TTYモードを有効にする。 ※Defaults
requirettyでOK

fn + option + F1/F2... : 切り替え

tty : 現在の使用

☐ また、セキュリティ上の問題から、sudoで利用できるパスを制限する。

ex.)

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
```

UFW

- Check the “UFW” program is properly installed on the VM and works properly.
“UFW”プログラムがVMに正しくインストールされ、正しく動作することを確認します。

sudo ufw status

- Ask the student for a basic explanation of UFW and the value of using it.

UFW の基本的な説明と使用する価値について、生徒に尋ねます。

UFWは、セキュリティを犠牲にすることなく、機器のファイアウォールを変更するためのインターフェースです。どのポートへの接続を許可し、どのポートを閉じるかを設定するために使用します。これは、SSHと組み合わせて、特定のポートを設定するのに便利です。

- List the active rules in UFW. A rule must exist for port 4242.

UFW のアクティブなルールをリストアップします。ポート 4242 に対してルールが存在する必要があります。

sudo ufw status

- Add a new rule to open port 8080. Check that this one has been added by listing the active rules.

ポート 8080 を開放するための新しいルールを追加します。アクティブなルールをリストアップして、これが追加されたことを確認します。

sudo ufw allow 8080

- Delete this new rule with the help of the student being evaluated.

評価される学生の助けを借りて、この新しいルールを削除します。

sudo ufw delete allow 8080

(sudo ufw delete 4)

(sudo ufw delete 2) 2回面倒

☐ UFWをインストールし、ポート4242だけオープンにする

SSH

- Check that the SSH service is properly installed on the VM, and is working properly.
SSHサービスがVMに正しくインストールされ、正しく動作していることを確認します。

sudo service ssh status *//check if its active and port 4242*

sudo service ssh status *//アクティブかどうか、ポート4242をチェックします。*

- Verify that the SSH service only uses port 4242.

SSH サービスがポート 4242 のみを使用していることを確認します。

cat /etc/ssh/sshd_config |grep port

- Ask the student for an explanation of what SSH is and the value of using it. (*answer: secure shell, allows 2 computers to securely talk to each other*)

SSH とは何か、それを使用することの価値について生徒に説明を求めます。(答え: セキュアシェル、2 台のコンピュータが互いに安全に通信することを可能にします)。

SSHは、クライアントとホスト間の認証メカニズムです。クライアントとホスト間のすべての通信が暗号化されるように、暗号化技術を使用します。MacやLinuxのユーザーは、SSHを使用してサーバーで作業するために端末を使用することができます。

☐ SSHのポート番号を4242に変更

#PermitRootLogin prohibit-password

→ PermitRootLogin no

→ reboot

- Ask the student to help you use SSH in order to log in with the newly created user. To do this, you can use a key or simple password, depending on the student being evaluated.

新しく作成したユーザーでログインするために、SSH を使用するのを手伝ってくれるように生徒に頼みます。これを行うには、評価される学生に応じて、鍵または単純なパスワードを使用することができます。

`ssh new_user@127.0.0.1 -p 4242`

- Make sure you cannot use SSH with the “root” user as stated in the subject.
お題にあるように、「root」ユーザーでSSHを使えないことを確認します。

`ssh root@127.0.0.1 -p 4242` *//should come up as permission denied*

`ssh root@127.0.0.1 -p 4242` *//permission deniedと出てくるはず。*

☐ rootでSSH接続できないようにする

Script Monitoring (questions for the student)

- **Ask the student how their script works and see their code for it.**

生徒が作成したスクリプトがどのように動作するのか、そのコードを見てもらいましょう。

Script inputted in the monitoring .sh file to display system information

システム情報を表示するための監視用.shファイルに入力されたスクリプト

`cd /usr/local/bin && vim monitoring.sh`

- **What is “cron”?**

cron とは何ですか？

Cronまたはcronジョブは、コマンドやスクリプトを毎日特定の間隔または特定の時刻に実行するようにスケジュールするためのコマンドラインユーティリティです。毎日特定の時刻にサーバーを再起動するように設定したい場合に便利です。

- `cd /usr/local/bin - monitoring.sh` を表示します。

- `sudo crontab -u root -e` ジョブを編集します。

change script to `*1 * * * sleep 30s && script path` - 30秒ごとに実行する場合は、この行を削除してジョブの実行を停止します。

- *How does the script run every 10 minutes from when the server starts?*

サーバーの起動時から10分ごとに実行されるスクリプトとは？

- Once correct functioning of the script is verified, ask the student to make sure the script runs with dynamic values correctly.

スクリプトが正しく機能することが確認できたら、動的な値でスクリプトが正しく実行されることを確認してもらってください。

`sudo crontab -u root -e (change 10 value to 1**)`**

`sudo crontab -u root -e (** 10の値を1***に変更)`**

- The student being evaluated should make the script stop running when the server has started up, without modifying the script itself. To check this, restart the VM.

評価される学生は、スクリプト自体を変更することなく、サーバーの起動時にスクリプトの実行を停止させる必要があります。これを確認するために、VMを再起動します。

`sudo cronstop`

```
sudo systemctl disable cron
```

`sudo cronstart`

```
sudo systemctl enable cron
```


- At startup, check if the script still exists in the same place, the rights have remained unchanged and that it has not been modified.

起動時に、

スクリプトが同じ場所に存在しているか、

権限が変更されていないか、

スクリプトが修正されていないか

を確認します。

sudo reboot

sudo crontab -u root -e

スクリプト作成

10分ごとにターミナルに情報を表示する

- ☐ オペレーティングシステムのアーキテクチャとそのカーネルバージョン
- ☐ 物理プロセッサの数
- ☐ 仮想プロセッサの数
- ☐ サーバー上の使用可能なRAMとその使用率
- ☐ サーバー上の使用可能なメモリとその使用率
- ☐ プロセッサの使用率（パーセント表示）
- ☐ 最後に再起動した日時が表示されます
- ☐ LVMがアクティブかどうか
- ☐ アクティブな接続の数
- ☐ サーバーを使用しているユーザーの数
- ☐ サーバーのIPv4アドレスとそのMACアドレス
- ☐ sudoプログラムで実行されたコマンドの数

b2b TODO-LIST

Born2beRoot Defense Checklist By Adrian Musso-Gonzalez (@amusso-g)
https://docs.google.com/document/d/1-BwCO0udUP7MhRh81Y681zz0BaIXtKFtte_FHJc6G4s/edit

該当の.utmファイルのパス
shasum Images/disk-0.qcow2
Preliminary tests Git repo cloned successfully. Git リポジトリのクローンに成功しました。**General instructions** Git repo contains a signature.txt file. Git リポジトリには signature.txt ファイルが含まれています。Check the signature against the students ".vdi" file, make sure it's identical. 生徒の ".vdi" ファイルと署名を照合し、同一であることを確認する。Clone VM || create a snapshot && open VM. VMのクローン | スナップショットを作成し、VMを開く。**Mandatory Part (Questions for the student)** **How does a virtual machine work and what is its purpose?** 仮想マシンはどのように動作し、その目的は何ですか？プログラムやアプリを実行するために、物理的なコンピュータの代わりにソフトウェアを使用するリソース。各VMは独自のオペレーティング・システムを持ち、別々に機能するため、1台のマシンに複数のVMを持つことができる。安全で独立した環境でアプリケーションをテストするために使用することができる。ソフトウェアを使って仮想ハードウェアをシミュレートし、ホストマシン上で実行することで機能する。**●ホスト型の仮想マシン** 物理マシンにWindowsやLinuxなどのOSをインストールして、その中に仮想ソフトウェアとなるアプリケーションをインストールして、仮想マシンを実現させる方式のこと。→既に利用しているパソコンやサーバーにも簡単にインストールできるため、導入しやすい。VMware Player Microsoft Virtual PC Oracle Virtual Box
●ハイパーバイザー型の仮想マシン ホストのOSを使わずに直接サーバーにソフトウェアをインストールして仮想マシンを実現する方式のこと。現在、最も主流な方式としてハイパーバイザー型が浸透している。→ホストOSが不要で直接ハードウェアを制御できるようになることから、仮想マシンの処理速度低下を最小限に抑えられる。VMware vSphere ESXi Citrix XenServer Hyper-V KVM
●コンテナ型の仮想マシン 物理マシンにWindowsやLinuxなどのホストOSをインストールして、コンテナ管理ソフトウェアをインストールして利用する方式。コンテナ型は、アプリケーションやソフトウェアを実行環境と共にコンテナイメージ（コンテナのテンプレートファイル）として包括することから、コンテナ型と呼ばれています。→コンテナイメージやソフトウェアそのものが軽量 Docker
The basic differences between CentOS and Debian? CentOS (rocky) と Debian の基本的な違い？Debian は、新しいバージョンがリリースされたときに、CentOS よりもずっと簡単にアップデート可能。Debian はよりユーザーフレンドリーで、多くのライブラリ、ファイルシステム、アーキテクチャーをサポートしている。また、カスタマイズのためのオプションもより多く存在。大規模なビジネスであれば、CentOS はより多くの商用機能を提供している点で優れている。*Their choice of operating system?* 彼らのOSの選択？インストールや設定が簡単だから、個人サーバーに最適。*If Debian: the difference between aptitude, apt*

and what APPArmor is. Debianの場合：aptitudeとaptの違い、APPArmorとは何か。

Aptitude は高レベルのパッケージマネージャであり、APT は他の高レベルのパッケージマネージャで利用できる低レベルのパッケージです。

Aptitude はより賢く、使っていないパッケージを自動的に削除したり、依存するパッケージのインストールを提案したりします。

Apt はコマンドラインで指示されたことのみを明示的に実行します。→ <https://ultra-genma.hateblo.jp/entry/2019/04/08/233718>※AppArmorとは？MAC (Mandatory

Access Control) セキュリティを提供するLinuxセキュリティシステムです。システム管理者がプロセスが実行できるアクションを制限することを可能にします。Debianにデフォルトで含まれています。aa-statusを実行して、実行されているかどうかを確認します。AppArmor とは、プログラム単位でMAC(Mandatory Access Control - 強制 アクセス制御)を行うためのセキュリティ機構のこと。MACとは、従来のファイルのパーミッションの設定等とは関係なく、強制的にアクセス制限を設けることができる。

AppArmor では、プログラム毎に、ファイルやソケットなどに対して行う ことのできる操作を明示的に指定し、それ以外の操作を行えなくすることができます。→セキュアな環境の構築が可能。 <https://www.usupi.org/sysad/220.html> **UFW** During the defense, a

script must display all information every 10 minutes. Its operation will be checked in detail later. 防御の間、スクリプトは10分ごとにすべての情報を表示しなければならない。その動作は後で詳しく確認する。All explanations are satisfactory (else evaluation stops here). すべての説明は満足のものである（そうでなければ評価はここでストップする）。

Simple setup Ensure that the machine does not have a graphical environment at launch. マシンが起動時にグラフィカルな環境でないことを確認します。Connect to VM as a created user (which isn't a root) 作成したユーザ (rootでない) でVMに接続する。Ensure the password follows the required policy (2 days min, 7, 30 days max). パスワードが必要なポリシーに従っていることを確認 (最低2日、7日、最大30日)

sudo chage -l username Evaluator checks UFW service is started. EvaluatorはUFWサービスが開始されていることを確認します。 **sudo ufw status** //look

for status: active Evaluator checks SSH service is started. SSHサービスが開始されていることを確認します。 **sudo systemctl status ssh** Evaluator checks the chosen

operating system (Debian or CentOS). 選択したオペレーティングシステム(DebianまたはCentOS)をチェックします。 **lsb_release -a || cat /etc/os-release** username -a User

The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to “sudo” and

“user42” groups. 評価対象者は、評価対象の学生のログイン名を持つユーザーが仮想マシンに存在することを要求します。追加されていることと、「sudo」「user42」グループに所属していることを確認してください。 **cat /etc/passwd | grep**

rwatanabgetent group sudogetent group user42自分のログイン名とするユーザーを作成し、user42とsudoグループに所属させるCreate new user (e.g. user42).新しいユーザー（例：user42）を作成します。**new_demoBorn2BeRootsudo adduser new_username**Assign a password of your choice, respecting subject rules.サブジェクトのルールを尊重しながら、好きなパスワードを割り当てる。**sudo usermod -aG sudo new_demogetent group sudo**Explanation from student explaining how to implement the password policy.パスワードポリシーの実行方法を説明する学生からの説明。パスワードのルールには、パスワード品質チェックライブラリを使用し、大文字と小文字、重複文字などのルールを設定するcommon-passwordファイルと、パスワードの有効期限ルール（30日など）を格納するlogin.defsファイルの2つのファイルがあります。**sudo nano /etc/login.defssudo nano /etc/pam.d/common-password**以下で確認！**sudo vi /etc/pam.d/common-password**↓ポリシーは以下を設定． password requisite pam_pwquality.so retry=3 minlen=10 ucredit=-1 dcredit=-1

※大文字・数字↓1の理由マイナス値で指定した場合、指定した文字種が指定した値の数含まれていなければならない

合、指定した文字種が指定した値の数含まれていなければならない

https://mseeeen.msen.jp/how-to-set-password-policy-in-centos7/#_minlenmaxrepeat=3reject_username difok=7 enforce_for_rootDebian 10 Buster : パスワードポリシーを設定する : Server Worldhttps://www.server-world.info/query?os=Debian_10&p=password
有効期限は30日最短利用日数は2日有効期限の7日前に警告メッセージを発する10文字以上大文字と数字を含む小文字最大連続文字数は3ユーザ名を含まない変更前に含まれる文字が変更後のパスワードに7文字以上含まれてはならないNormally there should be one or two modified files. If there is any problem, the evaluation stops here.通常、変更されるファイルは1つか2つであるはずです。もし問題があれば、評価はここで終了します。With the new user, ask the student to create a group named "evaluating" and assign it to the new user.新しいユーザで、"evalating" という名前のグループを作成し、新しいユーザに割り当てるよう学生に依頼します。**sudo groupadd evaluatingsudo usermod -aG evaluating your_new_username**Check if the new user belongs to the "evaluating" group.新しいユーザが "evaluating" グループに属しているかどうか確認します。**getent group evaluating**Ask the student to explain advantages of the password policy (beyond the fact that it is required for the project)パスワードポリシーの利点(プロジェクトに必要であるという事実以外)を説明するように学生に頼むAsk the student the advantages/disadvantages of the policy implementation.ポリシー導入のメリット/デメリットを生徒に質問する。**Hostname and partitions**Check the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).マシンのホスト名が次のように正しくフォーマットされていることを確認する: login42 (評価対象の学生のログイン)**hostnamectl**ホスト名をログイン名+42にす

るModify this hostname by replacing the login with yours, then restart VM.ログイン名を自分のものに置き換えてこのホスト名を変更し、VMを再起動します。 **sudo hostnamectl set-hostname new_hostname** **sudo vi /etc/hosts** → rwatanab42部分を新しいものに変える**sudo reboot**Note: If on restart, the hostname has not been updated, the evaluation stops here.Note: 再起動時にホスト名が更新されていない場合、評価はここで中断されます。Restore the machine to the original hostname, then restart VM.マシンを元のホスト名に復元してから、VMを再起動します。 **sudo hostnamectl set-hostname new_hostname** **sudo reboot**Ask the student being evaluated how to view the partitions for the VM.VM のパーティションを表示する方法を評価される学生に尋ねます。 **lsblk**Compare the output with the example given in the subject (if there are bonuses, refer to the bonus example).出力を課題文中の例と比較する(ボーナスがある場合は、ボーナス例を参照する)。Ask the student for a brief explanation of LVM and how it works.生徒にLVMとその動作について簡単に説明するように求める。Logical Volume Manager –論理ボリュームマネージャー - ストレージデバイス上のパーティションや論理ボリュームを簡単に操作することができる。暗号化LVMを使用してpdfにあるようなパーティションを作成**SUDO**Check that the “sudo” program is properly installed on the virtual machine.“sudo”プログラムが仮想マシンに適切にインストールされていることを確認します。 **dpkg -l | grep sudo**The student being evaluated shows assigning a new user to the “sudo” group.評価される学生は、新しいユーザを「sudo」グループに割り当てることを示しています。The subject imposes strict rules for sudo. The student being evaluated must explain the value and operation of sudo using examples of their choice.対象はsudoの厳格な規則を課しています。評価される学生は、選択した例を用いてsudoの価値と操作を説明する必要があります。 **sudo visudo** **ls**Second step, must show the implementation of the rules imposed by the subject.第二段階として、被験者が課したルールの実装を示す必要があります。Verify the “/var/log/sudo/” folder exists and has at least one file. Check the contents of the files in the folder, you should see a history of the commands used with sudo.**var/log/sudo/** フォルダが存在し、少なくとも 1 つのファイルがあることを確認する。フォルダ内のファイルの内容を確認し、あなたはsudoで使用されるコマンドの履歴が表示されるはずです。 **入力の履歴 : cat /var/log/sudo/sudo.log** **出力の記録 : sudo sudoreplay /var/log/sudo/00/00/01**Run a command via sudo. See if the file(s) in the “/var/log/sudo/” folder have been updated.sudoでコマンドを実行します。**var/log/sudo/** フォルダー内のファイルが更新されているかどうかを確認します。/etc/sudoersを直接編集してミスると大変らしいのでvisudoを使うsudo を使用した認証は、パスワードが正しくない場合、試行回数を 3 回に制限する。sudoの使用時にパスワードの間違いによるエラーが発生した場合、任意のカスタムメッセージを表示す

る。sudo を使用する各アクションを、入力と出力の両方をアーカイブする。ログファイルは /var/log/sudo/ フォルダに保存。Defaults iolog_dir="/var/log/sudo" セキュリティ上、TTYモードを有効にする。

※Defaults requirettyでOKfn + option + F1/F2... : 切り替えtty : 現在の使用また、セキュリティ上の問題から、sudoで利用できるパスを制限する。

ex.)/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

Shell**UFW**Check the "UFW" program is properly installed on the VM and works

properly."UFW"プログラムがVMに正しくインストールされ、正しく動作することを確認します。**sudo ufw status**Ask the student for a basic explanation of UFW and the

value of using it.UFW の基本的な説明と使用する価値について、生徒に尋ねます。UFW は、セキュリティを犠牲にすることなく、機器のファイアウォールを変更するためのインターフェースです。どのポートへの接続を許可し、どのポートを閉じるかを設定するために使用します。これは、SSHと組み合わせて、特定のポートを設定するのに便利です。List the active rules in UFW. A rule must exist for port 4242.UFW のアクティブなルールをリストアップします。ポート 4242 に対してルールが存在する必要があります。

sudo ufw statusAdd a new rule to open port 8080. Check that this one has been added by listing the active rules.ポート 8080 を開放するための新しいルールを追加します。アクティブなルールをリストアップして、これが追加されたことを確認します。**sudo**

ufw allow 8080Delete this new rule with the help of the student being evaluated.評価される学生の助けを借りて、この新しいルールを削除します。**sudo ufw delete allow**

8080(sudo ufw delete 4)(sudo ufw delete 2) 2回面倒UFWをインストールし、ポート 4242だけオープンにする**SSH**Check that the SSH service is properly installed on the

VM, and is working properly.SSHサービスがVMに正しくインストールされ、正しく動作していることを確認します。**sudo service ssh status** //check if its

active and port 4242**sudo service ssh status** //アクティブかどうか、ポート

4242をチェックします。Verify that the SSH service only uses port 4242.SSH サービスがポート 4242 のみを使用していることを確認します。**cat /etc/ssh/sshd_config**

lgrep portAsk the student for an explanation of what SSH is and the value of using it.

(answer: secure shell, allows 2 computers to securely talk to each other)SSH とは何か、

それを使用することの価値について生徒に説明を求めます。(答え: セキュアシェル、2 台のコンピュータが互いに安全に通信することを可能にします)。

SSHは、クライアントとホスト間の認証メカニズムです。クライアントとホスト間のすべての通信が暗号化されるように、暗号化技術を使用します。MacやLinuxのユーザーは、SSHを使用してサーバーで作業するために端末を使用することができます。SSHのポート番号を 4242に変更#PermitRootLogin prohibit-password → PermitRootLogin no → rebootAsk the

student to help you use SSH in order to log in with the newly created user. To do this,

you can use a key or simple password, depending on the student being evaluated.新しく作成したユーザーでログインするために、SSH を使用するのを手伝ってくれるように生徒に頼みます。これを行うには、評価される学生に応じて、鍵または単純なパスワードを使用することができます。ssh new_user@127.0.0.1 -p 4242 Make sure you cannot use SSH with the "root" user as stated in the subject.お題にあるように、

「root」ユーザーでSSHを使えないことを確認します。ssh root@127.0.0.1 -p 4242 //should come up as permission deniedssh root@127.0.0.1 -p 4242

//permission deniedと出てくるはず。rootでSSH接続できないようにする**Script**

Monitoring (questions for the student) Ask the student how their script works and see their code for it.生徒が作成したスクリプトがどのように動作するのか、そのコードを見てもらいましょう。

Script inputted in the monitoring .sh file to display system information システム情報を表示するための監視用.shファイルに入力されたスクリプト

cd /usr/local/bin && vim monitoring.sh What is "cron"? cron とは何ですか? Cron または cron ジョブは、コマンドやスクリプトを毎日特定の間隔または特定の時刻に実行するようにスケジュールするためのコマンドラインユーティリティです。毎日特定の時刻にサーバーを再起動するように設定したい場合に便利です。● cd /usr/local/bin - monitoring.sh を表示します。

● sudo crontab -u root -e ジョブを編集します。

change script to */1 * * * sleep 30s && script path - 30秒ごとに実行する場合は、この行を削除してジョブの実行を停止します。How does the script run every 10 minutes from when the server starts? サーバーの起動時から10分ごとに実行されるスクリプトとは?

Once correct functioning of the script is verified, ask the student to make sure the script runs with dynamic values correctly. スクリプトが正しく機能することが確認できたら、動的な値でスクリプトが正しく実行されることを確認してもらってください。sudo

crontab -u root -e (**change 10 value to 1**) sudo crontab -u root -e (**** 10の値を1***に変更) The student being evaluated should make the script stop running when the

server has started up, without modifying the script itself. To check this, restart the VM. 評価される学生は、スクリプト自体を変更することなく、サーバーの起動時にスクリプトの実行を停止させる必要があります。これを確認するために、VMを再起動します。

sudo cronstop sudo systemctl disable cron sudo cronstart sudo systemctl enable

cron At startup, check if the script still exists in the same place, the rights have remained unchanged and that it has not been modified. 起動時に、スクリプトが同じ場所に存在しているか、権限が変更されていないか、スクリプトが修正されていないかを確認しま

す。sudo reboot sudo crontab -u root -e スクリプト作成 10分ごとにターミナルに情報を表示するオペレーティングシステムのアーキテクチャとそのカーネルバージョン 物理プロセッサの数 仮想プロセッサの数 サーバー上の使用可能なRAMとその使用率 サーバ

ー上の使用可能なメモリとその使用率プロセッサの使用率（パーセント表示）最後に再起動した日時が表示されますLVMがアクティブかどうかアクティブな接続の数サーバーを使用しているユーザーの数サーバーのIPv4アドレスとそのMACアドレスsudoプログラムで実行されたコマンドの数