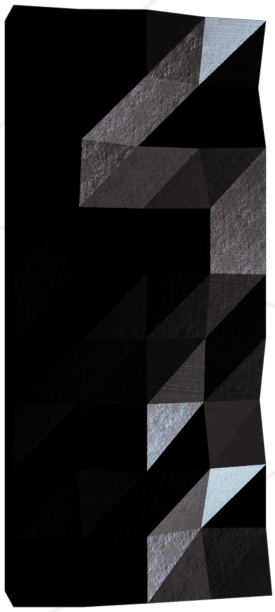
영어에서 한국어로 번역 - www.onlinedoctranslator.com



본투비루트

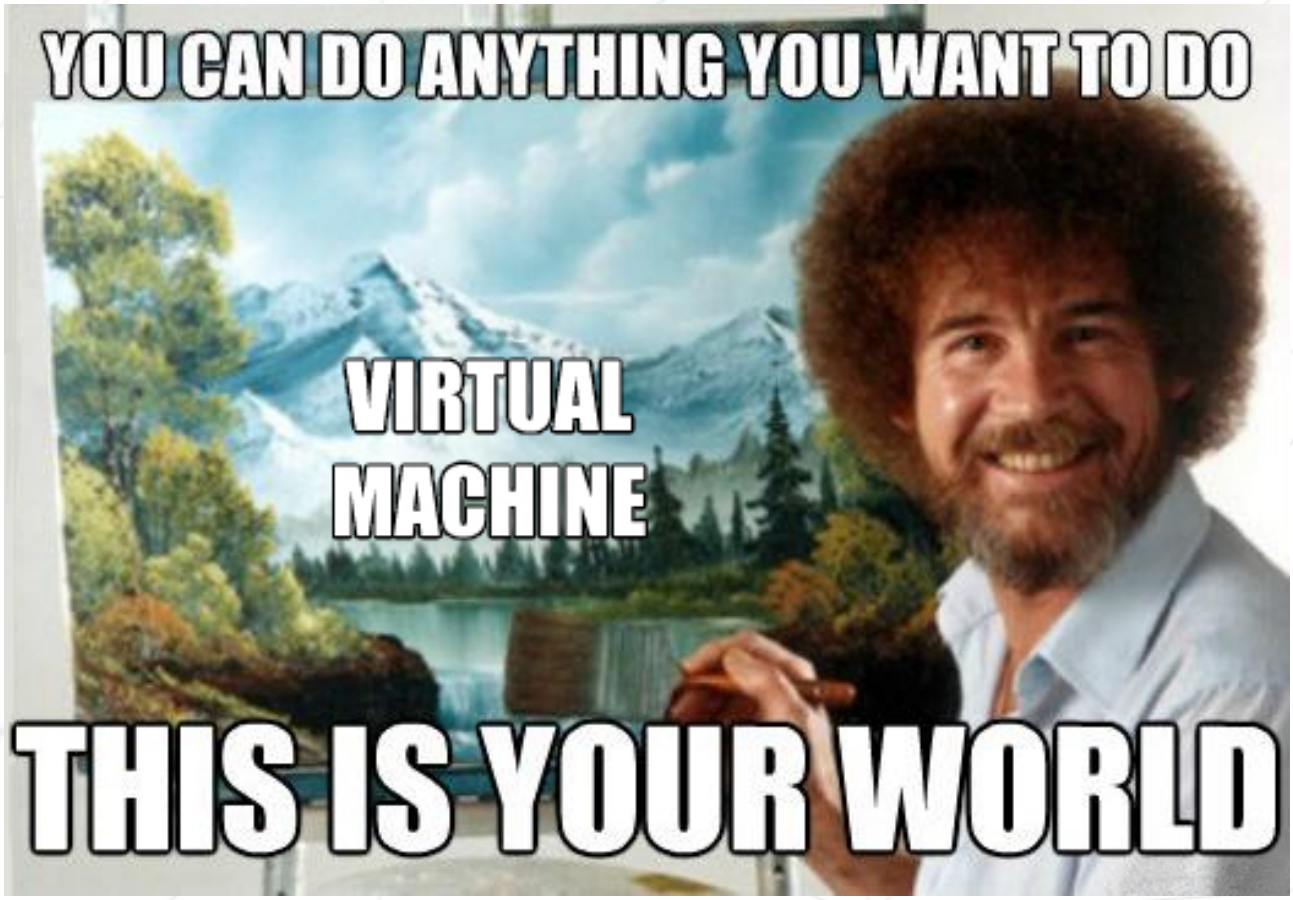
요약: 이 문서는 시스템 관리 관련 연습입니다.

버전: 1

내용물

1장

전문


YOU CAN DO ANYTHING YOU WANT TO DO
VIRTUAL
MACHINE
THIS IS YOUR WORLD

제2장

소개

이 프로젝트는 여러분에게 놀라운 가상화의 세계를 소개하는 것을 목표로 합니다.

에서 첫 번째 머신을 생성합니다.버추얼박스(또는UTM사용할 수 없다면버추얼박스) 특정 지침에 따라. 그런 다음 이 프로젝트가 끝나면 엄격한 규칙을 구현하면서 자신의 운영 체제를 설정할 수 있습니다.

제3장

일반 지침

- 의 사용버추얼박스(또는UTM사용할 수 없다면버추얼박스)필수입니다.
- 제출만 하면 됩니다서명.txt file 저장소의 루트에 있습니다. 여기에 컴퓨터의 가상 디스크 서명을 붙여넣어야 합니다. 자세한 내용은 제출 및 동료 평가로 이동하십시오.

제4장

필수 부분

이 프로젝트는 특정 규칙에 따라 첫 번째 서버를 설정하는 것으로 구성됩니다.

서버를 설정하는 문제이므로 최소한의 서비스만 설치하면 됩니다. 이러한 이유로 그래픽 인터페이스는 여기에서 사용되지 않습니다. 따라서 X.org 또는 기타 동등한 그래픽 서버를 설치하는 것은 금지되어 있습니다. 그렇지 않으면 등급은 0이 됩니다.

최신 안정 버전 중 하나를 운영 체제로 선택해야 합니다.데비안(테스트 없음/불안정) 또는 최신 안정 버전센트OS. 데비안시스템 관리를 처음 접하는 경우 적극 권장합니다.

CentOS 설정은 상당히 복잡합니다. 따라서 KDump를 설정할 필요가 없습니다. 그러나 SELinux는 시작 시 실행 중이어야 하며 해당 구성은 프로젝트의 요구 사항에 맞게 조정되어야 합니다. Debian용 AppArmor도 시작할 때 실행 중이어야 합니다.

다음을 사용하여 암호화된 파티션을 2개 이상 생성해야 합니다.LVM.다음은 예상되는 분할의 예입니다.

```
wil@wil:~$ lsblk
NAME                  MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                     8:0    0    8G  0 disk
├─sda1                  8:1    0  487M  0 part  /boot
├─sda2                  8:2    0    1K  0 part
└─sda5                  8:5    0  7.5G  0 part
  └─sda5_crypt        254:0    0  7.5G  0 crypt
    ├─wil--vg-root    254:1    0  2.8G  0 lvm   /
    ├─wil--vg-swap_1  254:2    0  976M  0 lvm   [SWAP]
    └─wil--vg-home    254:3    0  3.8G  0 lvm   /home
sr0                    11:0    1 1024M  0 rom
wil@wil:~$ _
```

방어하는 동안 선택한 운영 체제에 대한 몇 가지 질문을 받게 됩니다. 예를 들어 aptitude와 apt의 차이점, SELinux 또는 AppArmor가 무엇인지 알아야 합니다. 요컨대, 당신이 사용하는 것을 이해하십시오!

ㅏSSH서비스는 포트 4242에서만 실행됩니다. 보안상의 이유로 다음을 사용하여 연결할 수 없어야 합니다.SSH루트로.

SSH 사용은 방어 중에 새 계정을 설정하여 테스트합니다. 따라서 작동 방식을 이해해야 합니다.

다음을 사용하여 운영 체제를 구성해야 합니다.UFW 파이따라서 포트 4242만 열어 둡니다.

가상 머신을 시작할 때 방화벽이 활성화되어 있어야 합니다. CentOS의 경우 기본 방화벽 대신 UFW를 사용해야 합니다. 설치하려면 DNF가 필요할 것입니다.

- 그만큼호스트 이름의 가상 머신은 42로 끝나는 로그인이어야 합니다(예: wil42). 평가하는 동안 이 호스트 이름을 수정해야 합니다.
- 강력한 암호 정책을 구현해야 합니다.
- 설치하고 구성해야 합니다.수도엄격한 규칙을 따릅니다.
- 루트 사용자 외에도 사용자 이름으로 로그인한 사용자가 있어야 합니다.
- 이 사용자는 다음에 속해야 합니다.사용자42그리고수도여러 떼.

방어하는 동안 새 사용자를 만들고 그룹에 할당해야 합니다.

강력한 암호 정책을 설정하려면 다음 요구 사항을 준수해야 합니다.

- 비밀번호는 30일마다 만료되어야 합니다.
- 비밀번호 수정까지 허용되는 최소 일수는 2로 설정됩니다.

- 사용자는 비밀번호가 만료되기 7일 전에 경고 메시지를 받아야 합니다.
- 비밀번호는 10자 이상이어야 합니다. 대문자와 숫자를 포함해야 합니다. 또한 연속된 동일한 문자가 3개 이상 포함되어서는 안 됩니다.

- 암호에는 사용자 이름이 포함되어서는 안 됩니다.
- 다음 규칙은 루트 암호에 적용되지 않습니다. 암호는 이전 암호의 일부가 아닌 7자 이상이어야 합니다.
- 물론 루트 암호는 이 정책을 준수해야 합니다.

구성 파일을 설정한 후 루트 계정을 포함하여 가상 머신에 있는 계정의 모든 암호를 변경해야 합니다.

강력한 구성을 설정하려면수도그룹의 경우 다음 요구 사항을 준수해야 합니다.

- 다음을 사용하여 인증수도비밀번호가 올바르지 않은 경우 3번으로 제한됩니다.
- 사용 중 잘못된 비밀번호로 인한 오류가 발생한 경우 선택한 사용자 지정 메시지가 표시되어야 합니다.스도.
- 사용하는 각 작업수도입력과 출력 모두 보관해야 합니다. 로그 파일은 /var/log/sudo/폴더.
- 그만큼티티보안상의 이유로 모드를 활성화해야 합니다.
- 보안상의 이유로도 사용할 수 있는 경로수도제한해야 합니다. 예시:

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

마지막으로 라는 간단한 스크립트를 만들어야 합니다.모니터링.시.에 개발해야 합니다.세게 때리다.

서버 시작 시 스크립트는 10분마다 모든 터미널에 일부 정보(아래 나열)를 표시합니다.벽).배너는 선택 사항입니다. 오류가 표시되지 않아야 합니다.

스크립트는 항상 다음 정보를 표시할 수 있어야 합니다.

- 운영 체제 및 해당 커널 버전의 아키텍처입니다.
- 물리적 프로세서의 수입니다.
- 가상 프로세서의 수입니다.
- 서버에서 현재 사용 가능한 RAM 및 사용률(백분율)입니다.
- 서버의 현재 사용 가능한 메모리 및 사용률(백분율)입니다.
- 프로세서의 현재 사용률을 백분율로 표시합니다.
- 마지막 재부팅 날짜 및 시간입니다.
- LVM이 활성 상태인지 여부입니다.
- 활성 연결 수입니다.
- 서버를 사용하는 사용자 수입니다.
- 서버의 IPv4 주소와 해당 MAC(Media Access Control) 주소.
- 로 실행된 명령의 수수도프로그램.

방어하는 동안 이 스크립트가 어떻게 작동하는지 설명해야 합니다. 또한 수정하지 않고 중단해야 합니다. 크론을 살펴보십시오.

다음은 스크립트가 작동하는 방식의 예입니다.

```
root@wil (tty1) 의 브로드캐스트 메시지 (2021년 4월 25일 일요일 15:45:00):

        # 아키텍처: Linux wil 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
        # CPU 물리적 : 1
        # vCPU : 1
        # 메모리 사용량: 74/987MB(7.50%)
        # 디스크 사용량: 1009/2Gb(39%)
        # CPU 부하: 6.7%
        # 마지막 부팅: 2021-04-25 14:45
        # LVM 사용: 예
        # 연결 TCP : 1 ESTABLISHED
        # 사용자 로그: 1
        # 네트워크: IP 10.0.2.15 (08:00:27:51:9b:a5)
        # 수도 : 42cmd
```

다음은 주제의 요구 사항 중 일부를 확인하는 데 사용할 수 있는 두 가지 명령입니다.

을 위한센트OS:

```
[root@wil ~]# head -n 2  /etc/os-release
NAME="CentOS Linux"
VERSION="8"
[root@wil ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      32
[root@wil ~]# ss -tunlp
Netid State  Recv-Q  Send-Q   Local Address:Port   Peer Address:Port
tcp   LISTEN 0       128           0.0.0.0:4242        0.0.0.0:*     users:(("sshd",pid=822,fd=5))
tcp   LISTEN 0       128              [::]:4242           [::]:*     users:(("sshd",pid=822,fd=7))
[root@wil ~]# ufw status
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)

[root@wil ~]# _
```

을 위한데비안:

```
root@wil:~# head -n 2 /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
root@wil:/home/wil# /usr/sbin/aa-status
apparmor module is loaded.
root@wil:/home/wil# ss -tunlp
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:Port

tcp   LISTEN 0      128          0.0.0.0:4242       0.0.0.0:*     users:(("sshd",pid=523,fd=3))
tcp   LISTEN 0      128             [::]:4242          [::]:*     users:(("sshd",pid=523,fd=4))
root@wil:/home/wil# /usr/sbin/ufw status
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)
```

제5장

보너스 부분

보너스 목록:

- 파티션을 올바르게 설정하여 아래와 유사한 구조를 얻습니다.

```
# lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                     8:0    0  30.8G  0 disk
├─sda1                  8:1    0   500M  0 part  /boot
├─sda2                  8:2    0     1K  0 part
└─sda5                  8:5    0  30.3G  0 part
  └─sda5_crypt        254:0    0  30.3G  0 crypt
    ├─LVMGroup-root   254:1    0    10G  0 lvm   /
    ├─LVMGroup-swap   254:2    0   2.3G  0 lvm   [SWAP]
    ├─LVMGroup-home   254:3    0     5G  0 lvm   /home
    ├─LVMGroup-var    254:4    0     3G  0 lvm   /var
    ├─LVMGroup-srv    254:5    0     3G  0 lvm   /srv
    ├─LVMGroup-tmp    254:6    0     3G  0 lvm   /tmp
    └─LVMGroup-var--log 254:7  0     4G  0 lvm   /var/log
sr0                    11:0    1  1024M  0 rom
```

- lighttpd, MariaDB 및 PHP 서비스를 사용하여 기능적인 WordPress 웹 사이트를 설정합니다.
- 유용하다고 생각되는 서비스를 설정하세요(NGINX/Apache2 제외!). 방어하는 동안 선택을 정당화해야 합니다.

보너스 부분을 완료하기 위해 추가 서비스를 설정할 수 있습니다. 이 경우 필요에 맞게 더 많은 포트를 열 수 있습니다. 물론 UFW 규칙은 그에 따라 조정되어야 합니다.

필수 부분이 PERFECT인 경우에만 보너스 부분이 평가됩니다. Perfect는 필수 부분이 완벽하게 수행되어 오작동 없이 작동함을 의미합니다. 모든 필수 요구 사항을 통과하지 못한 경우 보너스 부분은 전혀 평가되지 않습니다.

제6장

제출 및 동료 평가

제출만 하면 됩니다서명.txt fi당신의 뿌리에 르힘내저장소. 여기에 컴퓨터의 가상 디스크 서명을 붙여넣어야 합니다. 이 서명을 얻으려면 먼저 기본 설치 폴더(VM이 저장되는 폴더)를 열어야 합니다.

- 윈도우: %HOMEDRIVE%%HOMEPATH%\VirtualBox VM\
- 리눅스: ~/VirtualBox VM/
- MacM1: ~/라이브러리/컨테이너/com.utmapp.UTM/Data/Documents/
- 맥OS: ~/VirtualBox VM/

그런 다음 "에서 서명을 검색합니다.vdi "fi르(또는 ".qcow2~을 위한UTM'사용자)의 가상 머신샤1체재. 다음은 4가지 명령 예입니다.centos_serv.vdi 파일:

- 윈도우:certUtil -hashfile centos_serv.vdi sha1
- 리눅스:sha1sum centos_serv.vdi
- Mac M1의 경우:shasum Centos.utm/Images/disk-0.qcow2
- 맥 OS:shasum centos_serv.vdi

다음은 어떤 종류의 출력을 얻을 수 있는지 보여주는 예입니다.

- 6e657c4619944be17df3c31faa030c25e43e40af

가상 머신의 서명은 첫 번째 평가 후에 변경될 수 있습니다. 이 문제를 해결하기 위해 가상 머신을 복제하거나 상태 저장을 사용할 수 있습니다.

물론 Git 저장소에서 가상 머신을 켜는 것은 금지되어 있습니다. 방어하는 동안 signature.txt 파일의 서명은 가상 머신의 서명과 비교됩니다. 두 가지가 동일하지 않은 경우 등급은 0입니다.