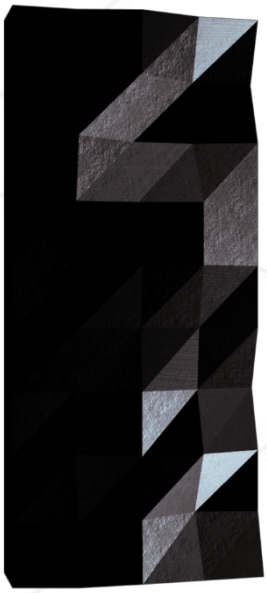


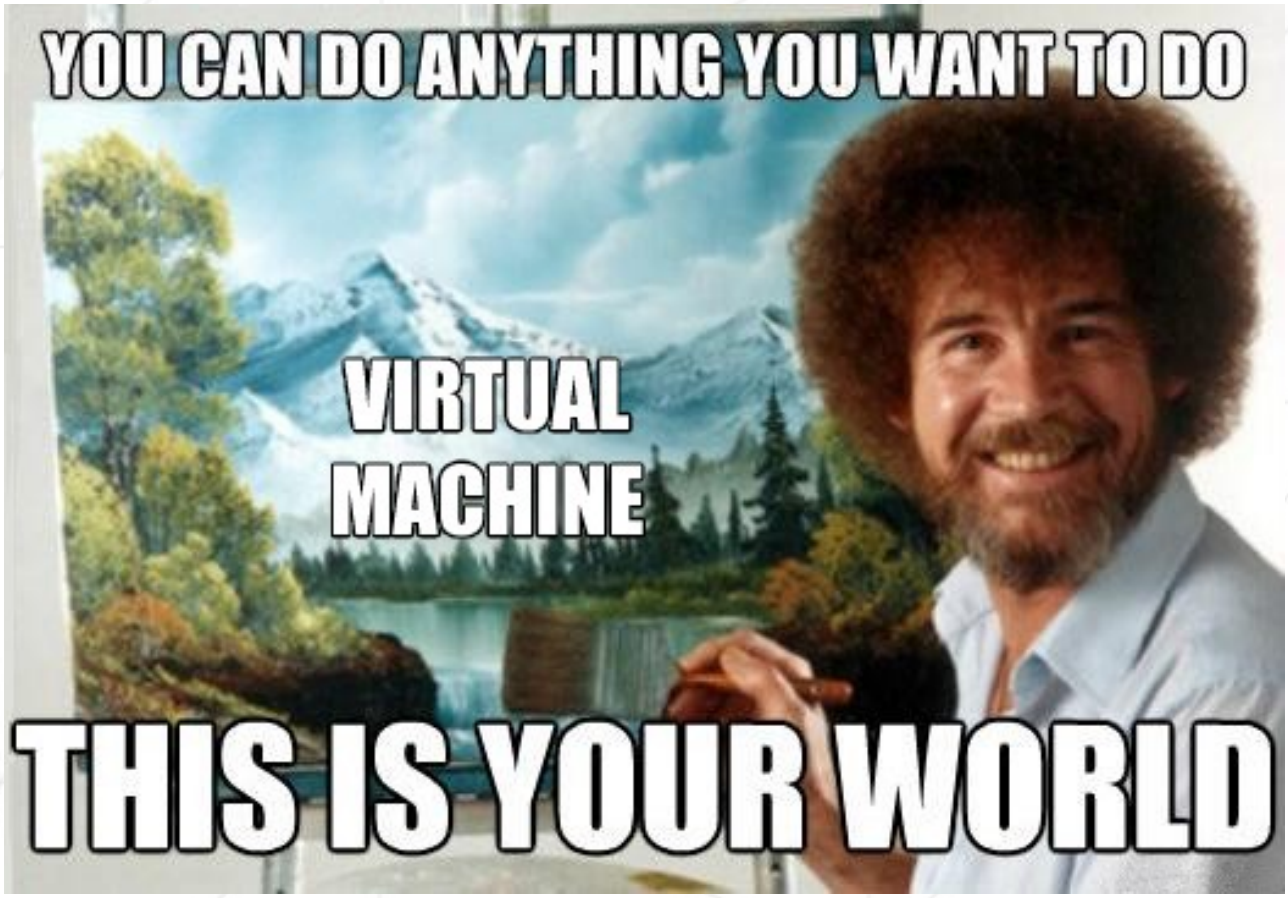
Born2beRoot

요약: 이 문서는 시스템 관리와 관련된 연습 문제입니다.

버전: 3.2

콘텐츠

제1장 서문


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

2장 소개

이 프로젝트는 가상화의 놀라운 세계를 소개하는 것을 목표로 합니다.

특정 지침에 따라 가상 박스(또는 가상 박스를 사용할 수 없는 경우 UTM)에서 첫 번째 머신을 생성합니다. 그런 다음 이 프로젝트가 끝나면 엄격한 규칙을 구현하면서 자신만의 운영 체제를 설정할 수 있습니다.

제3장 일반 지침

- 가상 박스(또는 가상 박스를 사용할 수 없는 경우 UTM)를 반드시 사용해야 합니다.
- 리포지토리의 루트에 서명.txt 파일만 제출하면 됩니다. 이 파일에 컴퓨터의 가상 디스크 서명을 붙여넣어야 합니다. 자세한 내용은 제출 및 동료 평가로 이동하세요.

4장 필수 부분

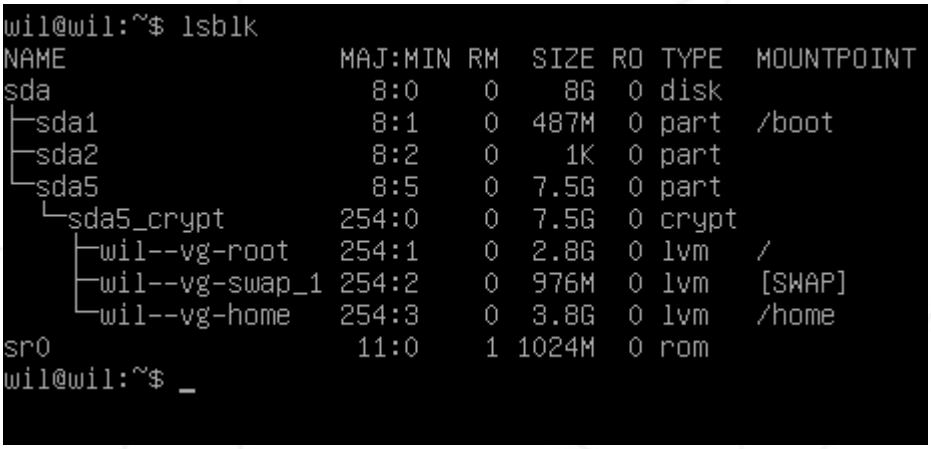
이 프로젝트는 특정 규칙에 따라 첫 번째 서버를 설정하는 것으로 구성됩니다.

서버를 설정하는 문제이므로 최소한의 서비스만 설치하게 됩니다. 따라서 여기에서는 그래픽 인터페이스는 사용할 수 없습니다. 따라서 X.org 또는 기타 동등한 그래픽 서버를 설치하는 것은 금지되어 있습니다. 그렇지 않으면 성적이 0점이 됩니다.

운영체제로는 최신 안정 버전인 Debian(테스트 없음/불안정) 또는 최신 안정 버전인 Rocky 중 하나를 선택해야 합니다. 시스템 관리가 처음이라면 Debian을 적극 권장합니다.

Rocky 설정은 매우 복잡합니다. 따라서 KDump를 설정할 필요는 없습니다. 그러나 시작 시 SELinux가 실행 중이어야 하며 프로젝트의 요구 사항에 맞게 구성을 조정해야 합니다. Debian용 AppArmor도 시작 시 실행 중이어야 합니다.

LVM을 사용하여 암호화된 파티션을 2개 이상 만들어야 합니다. 아래는 예상되는 파티션의 예입니다:



방어하는 동안 선택한 운영 체제에 대한 몇 가지 질문을 받게 됩니다. 예를 들어, apt와 apt의 차이점이나 SELinux 또는 AppArmor가 무엇인지 알아야 합니다. 요컨대, 자신이 사용하는 것을 이해해야 합니다!

가상 머신의 필수 포트 4242에서 SSH 서비스가 실행됩니다.
보안상의 이유로 SSH를 루트로 사용하여 연결할 수 없어야 합니다.

새 계정을 설정하여 방어하는 동안 SSH 사용을 테스트합니다. 따라서 어떻게 작동하는지 이해해야 합니다.

가상 머신에 포트 4242만 열어두고 UFW(또는 Rocky의 경우 방화벽) 방화벽으로 운영 체제를 구성해야 합니다.

가상 머신을 시작할 때 방화벽이 활성화되어 있어야 합니다. Rocky의 경우 UFW 대신 방화벽을 사용해야 합니다.

- 가상 머신의 호스트 이름은 42로 끝나는 로그인 이름이어야 합니다(예 : wil42). 평가 중에 이 호스트 이름을 수정해야 합니다.
- 강력한 비밀번호 정책을 구현해야 합니다.
- 엄격한 규칙에 따라 sudo를 설치하고 구성해야 합니다.
- 루트 사용자 외에 로그인한 사용자 아이디를 사용자 아이디로 사용하는 사용자가 있어야 합니다.
- 이 사용자는 user42 및 sudo 그룹에 속해야 합니다.

방어하는 동안 새 사용자를 만들어 그룹에 할당해야 합니다.

강력한 비밀번호 정책을 설정하려면 다음 요구 사항을 준수해야 합니다:

- 비밀번호는 30일마다 만료되어야 합니다.
- 비밀번호를 수정할 수 있는 최소 일수는 2일로 설정됩니다.

- 사용자는 비밀번호가 만료되기 7일 전에 경고 메시지를 받아야 합니다.
- 비밀번호는 10자 이상이어야 합니다. 대문자, 소문자, 숫자를 포함해야 합니다. 또한 동일한 문자가 3개 이상 연속으로 포함되지 않아야 합니다.

- 비밀번호에는 사용자 이름이 포함되어서는 안 됩니다.
- 루트 비밀번호에는 다음 규칙이 적용되지 않습니다. 비밀번호에는 이전 비밀번호에 포함되지 않은 7자 이상의 문자가 포함되어야 합니다.
- 물론 루트 비밀번호는 이 정책을 준수해야 합니다.

구성 파일을 설정한 후에는 루트 계정을 포함하여 가상 머신에 있는 모든 계정의 비밀번호를 변경해야 합니다.

sudo 그룹에 대한 강력한 구성을 설정하려면 다음 요구 사항을 준수해야 합니다:

- 비밀번호를 잘못 입력한 경우 sudo를 사용한 인증은 3회 시도로 제한해야 합니다.
- sudo를 사용할 때 잘못된 비밀번호로 인한 오류가 발생하면 원하는 사용자 지정 메시지를 표시해야 합니다.
- sudo를 사용한 각 작업은 입력과 출력 모두 보관해야 합니다. 로그 파일은 /var/log/sudo/ 폴더에 저장해야 합니다.
- 보안상의 이유로 TTY 모드를 활성화해야 합니다.
- 보안상의 이유로 sudo에서 사용할 수 있는 경로도 제한해야 합니다. 예시: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

마지막으로 모니터링.sh라는 간단한 스크립트를 만들어야 합니다. 이 스크립트는 bash에서 개발해야 합니다.

서버가 시작되면 스크립트가 10분마다 모든 테라에 몇 가지 정보(아래 나열됨)를 표시합니다(벽을 보세요). 배너는 선택 사항입니다. 오류가 표시되지 않아야 합니다.

스크립트는 항상 다음 정보를 표시할 수 있어야 합니다:

- 운영 체제의 아키텍처 및 커널 버전입니다.
- 물리적 프로세서 수입니다.
- 가상 프로세서 수입니다.
- 서버의 현재 사용 가능한 RAM과 백분율로 표시된 사용률입니다.
- 서버의 현재 사용 가능한 메모리와 백분율로 표시된 사용률입니다.
- 프로세서의 현재 사용률을 백분율로 표시합니다.
- 마지막으로 재부팅한 날짜와 시간입니다.
- LVM이 활성화되어 있는지 여부.
- 활성 연결 수입니다.
- 서버를 사용하는 사용자 수입니다.
- 서버의 IPv4 주소와 해당 서버의 MAC(미디어 액세스 제어) 주소입니다.
- sudo 프로그램으로 실행한 명령의 수입니다.

방어하는 동안 이 스크립트가 어떻게 작동하는지 설명하라는 요청을 받게 됩니다. 또한 스크립트를 수정하지 않고 중단해야 합니다. 크론을 살펴보세요.

다음은 스크립트가 어떻게 작동할 것으로 예상되는지 보여주는 예시입니다:

```
(Sun Apr 25 15:45:00 2021) (tty1) (으)로부터 root@wil (으)로부터 방송 메시지:

    #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(49%)
    #CPU 부하: 6.7%
    #마지막 부팅: 2021-04-25 14:45
    #LVM 사용: 예
    #연결 TCP : 1 설정됨 #사용자 로그: 1
    #네트워크: IP 10.0.2.15 (08:00:27:51:9b:a5)
    #수도 : 42 cmd
```

다음은 피사체의 일부 요구 사항을 확인하는 데 사용할 수 있는 두 가지 명령어입니다:

록키의 경우

```
[root@wil wil]# head -n 2 /etc/os-release
NAME="Rocky Linux"
VERSION="8.7 (Green Obsidian)"
[root@wil 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:      33
[root@wil wil]# ss -tunlp
Netid State  Recv-Q Send-Q  Local Address:Port   Peer Address:Port Process
tcp   LISTEN 0      128           0.0.0.0:4242        0.0.0.0:*     users:(("sshd",pid=28429,fd=6))
tcp   LISTEN 0      128              [::]:4242           [::]:*     users:(("sshd",pid=28429,fd=4))
[root@wil wil]# firewall-cmd --list-service
ssh
[root@wil wil]# firewall-cmd --list-port
4242/tcp
[root@wil wil]# firewall-cmd --state
running
[root@wil wil]# _
```

데비안의 경우:

```
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)
```

5장 보너스 부분

보너스 목록:

- 파티션을 올바르게 설정하여 아래 그림과 비슷한 구조가 되도록 합니다:

```
# 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
```

- 다음과 같은 서비스로 기능적인 워드프레스 웹사이트를 설정하세요: lighttpd, Mari- aDB, PHP.
- 유용하다고 생각되는 서비스를 설정합니다(NGINX / Apache2 ex- cluded!). 방어하는 동안 자신의 선택을 정당화해야 합니다.

보너스 부분을 완료하기 위해 추가 서비스를 설정할 수 있습니다. 이 경우 필요에 따라 더 많은 포트를 열 수 있습니다. 물론 UFW/방화벽 규칙을 그에 맞게 조정해야 합니다.

보너스 부분은 필수 부분이 완벽한 경우에만 평가됩니다. 완벽하다는 것은 필수 부분을 완벽하게 완료하고 오작동 없이 작동한다는 의미입니다. 모든 필수 요건을 통과하지 못한 경우 보너스 부분은 전혀 평가되지 않습니다.

제6장

제출 및 동료 평가

Git 리포지토리의 루트에 signature.txt 파일만 제출하면 됩니다. 이 파일에 머신의 가상 디스크 서명을 붙여넣어야 합니다. 이 서명을 받으려면 먼저 기본 설치 폴더(VM이 저장된 폴더)를 열어야 합니다:

- Windows: %홈드라이브%%홈패스%\VirtualBox VM\
- Linux: ~/VirtualBox VMs/
- MacM1: ~/Library/Containers/com.utmapp.UTM/Data/Documents/
- MacOS: ~/VirtualBox VMs/

그런 다음 가상 머신의 ".vdi" 파일(또는 UTM'사용자의 경우 ".qcow2)에서 sha1 형식의 서명을 검색합니다. 다음은 rocky_serv.vdi 파일에 대한 4가지 명령 예제입니다:

- Windows: certUtil -해시 파일 rocky_serv.vdi sha1
- Linux: sha1sum rocky_serv.vdi
- Mac M1의 경우: shasum rocky.utm/Images/disk-0.qcow2
- MacOS: shasum rocky_serv.vdi

이것은 어떤 종류의 출력을 얻을 수 있는지 보여주는 예입니다:

- 6e657c4619944be17df3c31faa030c25e43e40af

첫 번째 평가 후에는 가상 머신의 서명이 변경될 수 있다는 점에 유의하세요.
이 문제를 해결하려면 가상 머신을 복제하거나 저장 상태를 사용할 수 있습니다
.

물론 Git 리포지토리에서 가상 머신을 제출하는 것은 금지되어 있습니다. 방어하는 동안 signature.txt 파일의 서명이 가상 머신의 서명과 비교됩니다. 둘이 동일하지 않으면 성적이 0점이 됩니다.

```
0010 01 11 111 001 000   11 01      101 0000 01 1 1010 111 11 0 000
 011 00 1        00001  0   01 0100 1 0 010 10 01 1 0   0001 0 010 000
         0000
00 111      10111      0010001100 001100 001100
```