[palm] Write-Up

작성자	김경민
분석 일자	2024.05.10
작성 일자	2024.05.11
분석 대상	
문서 버전	3.0
작성자 E-mail	rlarudals877@gmail.com

목차

1. 문제

URL	https://dreamhack.io/wargame/challenges/183
문제 내용	드림회사에서 운영 중인 서버가 해킹이 된 징후를 포착했습니다. 자세한 것은 알 수 없지만, 악성 코드는 중앙 서버를 통해 개발자 PC로 침투했고, 그 결과 개발자 PC에서 **로그인을 할 때 마다 네트워크 데이터**에 민감한 로그인 정보가 유출되고 있음을 파악했습니다. 침투가 완료된 PC에 접속하여 악성 코드를 분석하고 침투에 사용된 파일을 찾아 Flag를 찾아주세요!
문제 파일	-
문제 유형	네트워크 포렌식
난이도	2 / 3

2. 분석 도구

도구명	다운로드 링크	Version
-	-	-
-	-	-
-	-	-

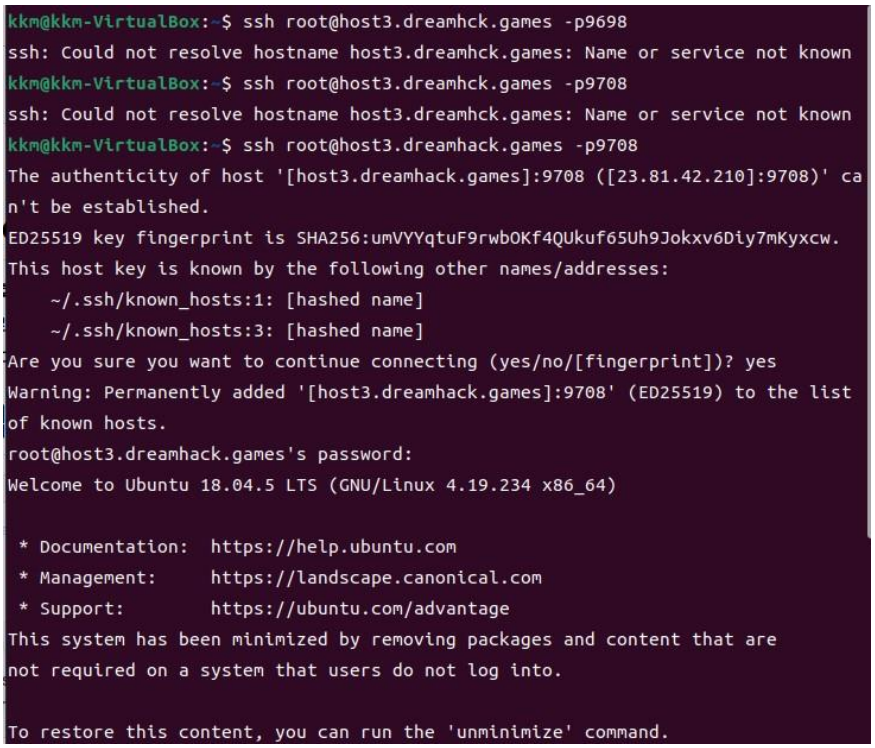
3. 환경

OS
Ubuntu 22.04

4. Write-Up

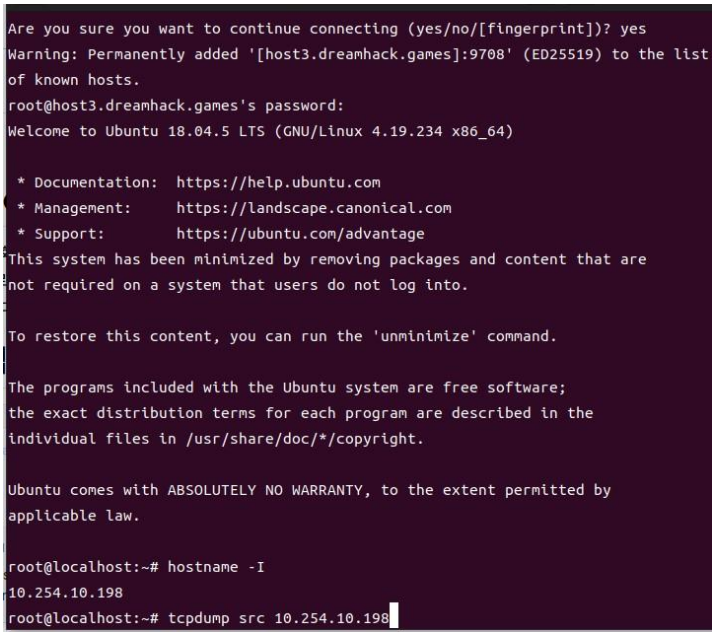
파일명	-
용량	-
SHA256	-
Timestamp	-

1. 일단 dreamhack 에서 서버를 열고 해당 서버로 접속해주었다.



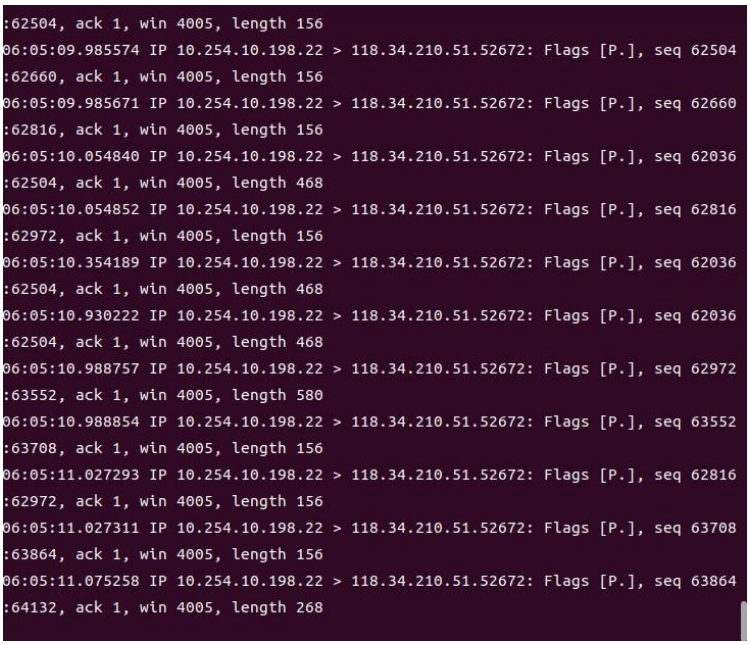
[사진 1] 서버 접속하기

2. 그리고 IP 를 확인해주었고 얻은 IP 주소를 출발지로 하여 tcpdump 명령어를 사용해 패킷을 잡으려고 했다.



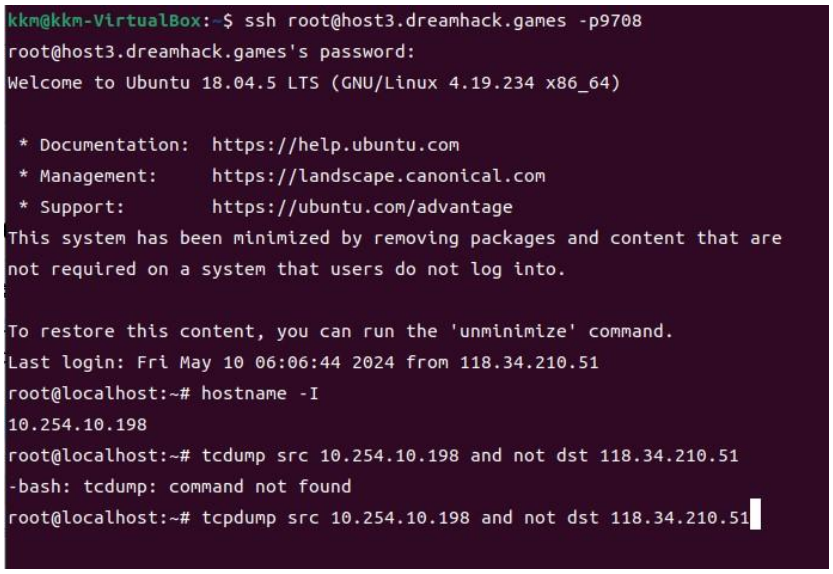
[사진 2] 패킷 잡기

3. 위의 명령어를 입력하니 특정 경로로 불필요한 패킷이 너무 많이 보였다. 자세히 보니 118.34.210.51 에서 수도 없이 패킷을 보내 제대로 확인할 수가 없었다. (참고로 문제에서 로그인 할 때 마다 네트워크 데이터에 민감한 로그인 정보가 유출됐다고 하니 이때 발생되는 패킷은 로그인 시에 발생하는 네트워크 패킷이다.)



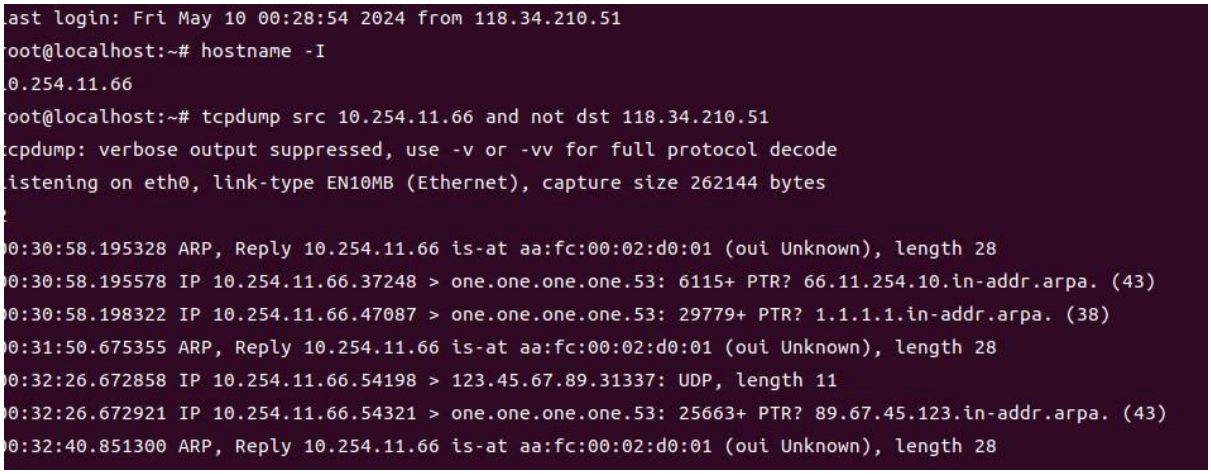
[사진 3] 패킷 발생 + 불필요한 패킷이 많이 보임

4. 따라서 118.34.210.51을 제외한 패킷을 캡처했다.



[사진 4] 필터링해서 패킷 갭처

5. 그랬더니 몇 개의 패킷이 잡히는데, 그 중 UDP 31337 에 보내는 패킷 IP 를 확인했다. 참고로 31337 포트는 백도어 또는 악성코드에서 많이 사용되는 포트이다. 따라서 로그인 시 위 IP 로 로그인 정보가 유출되었다고 추측하였다. (이때 IP 는 123.45.67.89)



[사진 5] 이상한 IP 확인

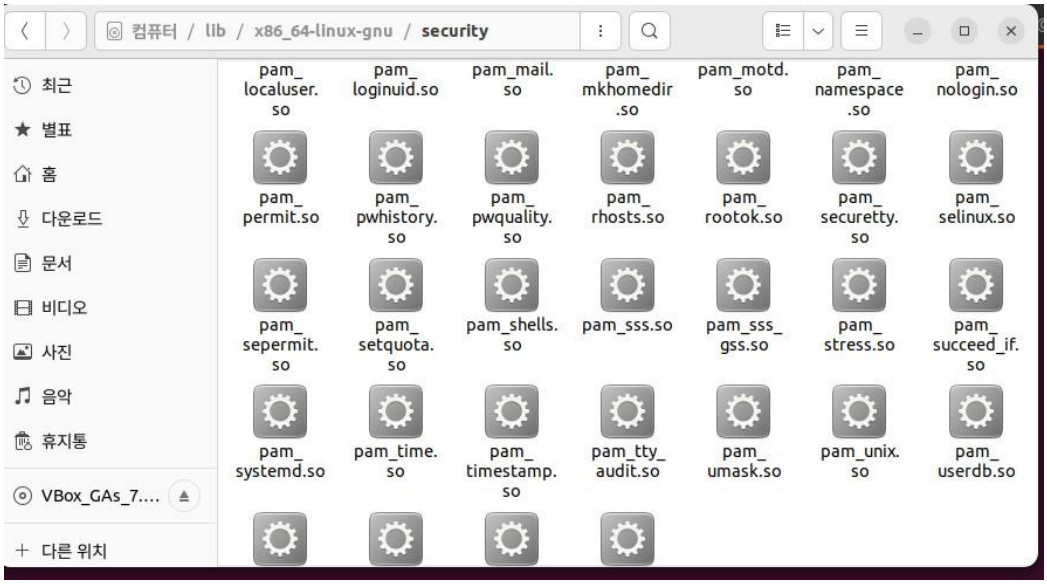
6. 따라서 grep 명령어를 이용해서 리눅스 시스템에서 공격자가 침투한 경우 조작했을 가능성이 높은 /var, /log, /etc, /home, /lib 등의 폴더로 위의 ip를 포함하고 있는 파일들을 검색하였고 /lib 의 pam_unix.so 파일에서 123.45.67.89가 검색된다는 것을 알 수 있었다.

```
kkm@kkm-VirtualBox:~$ ssh root@host3.dreamhack.games -p17676
root@host3.dreamhack.games's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.19.234 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri May 10 00:32:27 2024 from 118.34.210.51
root@localhost:~# grep '123.45.67.89' -r /lib
Binary file /lib/x86_64-linux-gnu/security/pam_unix.so matches
root@localhost:~#
```

[사진 6] 이상한 ip를 가지고 있는 파일 확인



[사진 7] 해당 파일 위치 확인

7. 처음에는 IDA 를 이용해서 파일을 디코딩 하려고 하였으나 IDA 에서 .so 파일을 열수가 없었다. 근데 flag 는 문자열 형식이니 strings 명령어를 이용해서 해당 파일을 문자열로 출력하였다. 그 결과 여러 문자열이 나왔고 인코딩된 flag 를 찾을 수 있었다. 따라서 base64 로 인코딩 된 데이터를 디코딩하여서 flag 를 확인하였다.

```
Try 'grep --help' for more information.
root@localhost:~# grep '123.45.67.89' -r /lib
Binary file /lib/x86_64-linux-gnu/security/pam_unix.so matches
root@localhost:~# strings /lib/x86_64-linux-gnu/security/pam_unix.so
`^B
__gmon_start__
_ITM_deregisterTMCloneTable
_ITM_registerTMCloneTable
__cxa_finalize
calloc
```

[사진 8] pam_unix 파일을 문자열로 출력

```
Password:
-UN*X-PASS
%d:%s:%s
123.45.67.89
auth could not identify password for [%s]
REh7c29tZXRoaW5nX2hpZGRlbl9pbnNpZGVfbXlfcGFsbX0=No password supplied
Password unchanged
Can not get username
/etc/security/opasswd
bad authentication token
 or NIS
 not
```

[사진 9] 인코딩 된 flag 찾음

```
root@localhost:~# echo REh7c29tZXRoaW5nX2hpZGRlbl9pbnNpZGVfbXlfcGFsbX0= | base6
4 -d
DH{something_hidden_inside_my_palm}root@localhost:~#
```

[사진 10] 디코딩된 flag

5. Flag

DH{something_hidden_inside_my_palm}

6. 별도 첨부

7. Reference

- https://scorchingnraining.tistory.com/entry/DreamHack-palm-%EB%AC%B8%EC%A0%9C-%ED%92%80%EC%9D%B4forensicnabi
- https://velog.io/@gl24/palm
- https://jc0626.tistory.com/entry/Dreamhack-palm-%EB%AC%B8%EC%A0%9C-%ED%92%80%EC%9D%B4