

작성자	류나연
분석 일자	2024.05.10
작성 일자	2024.05.10
분석 대상	evidence.tar
문서 버전	2
작성자 E-mail	<a href="mailto:01star01ek@gmail.com">01star01ek@gmail.com</a>

## 0. 목차

1. 문제 .....	3
-------------	---

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag.....7

6. 별도 첨부 .....8

7. Reference .....9

1. 문제

URL	<a href="http://suninatas.com/challenge/web14/web14.asp">http://suninatas.com/challenge/web14/web14.asp</a>
문제 내용	<p>Suninatas의 password를 찾아내는 문제.</p> <p>주어진 파일을 download시 압축된 tar 파일에 password 파일과 shadow 파일이 있습니다. 해당 파일에서 password를 찾아내면 됩니다.</p>
문제 파일	<div>  <div>evidence.tar</div> </div>
문제 유형	패스워드 크래킹
난이도	1 / 5

2. 분석 도구

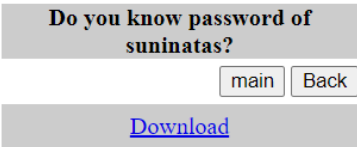
도구명	다운로드 링크	Version
John The Ripper	<a href="https://www.openwall.com/john/">https://www.openwall.com/john/</a>	1.8.0-4ubuntu3
Hxd	<a href="https://mh-nexus.de/en/downloads.php?product=HxD20">https://mh-nexus.de/en/downloads.php?product=HxD20</a>	2.5.0.0

3. 환경

OS
Windows 11, ubuntu 2204.3.49.0

## 4. Write-Up

파일명	evidence.tar
용량	10.0kb
SHA256	fcf3ac52e63a3b5c856137feef05a8e2f7f1592a41c9a7072ca66e4533671a0f
Timestamp	2012-03-28 11:33:32



[사진 1] 문제 사진

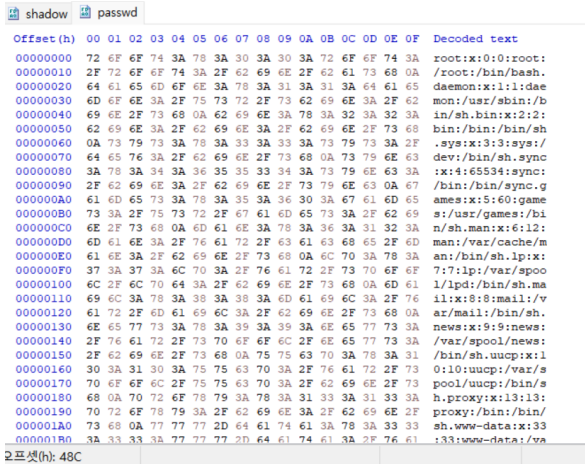
Suninatas 의 14 번 문제는 사진 1 번과 같이 password 를 찾아 내는 문제입니다.

Download의 문자를 따라 하이퍼링크를 클릭하면 tar 형식의 파일을 다운로드 할 수 있습니다.



[사진 2] tar 파일

해당 파일을 확인해보면 사진2를 통해 보이는 것처럼 shadow명의 파일과 passwd명의 파일이 있음을 확인할 수 있습니다. Bin/shadow와 Bin/passwd가 떠오르는 파일 이름입니다.



[사진 3] HxD를 통해 확인한 파일들

## [WHS-2] .iso

정확한 확인을 위하여 HxD로 해당 파일에 적혀진 내용을 확인하였습니다. 이를 통해 확인해보면 추측과 같이 **bin/shadow와 bin/passwd의 내용임을 알 수 있습니다.** 이에 따라 편리하게 확인하기 위해 Decode text의 내용을 복사 붙여넣기로 메모장에 붙여 확인해보았습니다.

```
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:103:108::/var/lib/landscape:/bin/false
messagebus:x:104:112::/var/run/dbus:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
mysql:x:105:113::/var/lib/mysql:/bin/false
avahi:x:106:114::/var/run/avahi-daemon:/bin/false
snort:x:107:115:Snort IDS:/var/log/snort:/bin/false
statd:x:108:65534::/var/lib/nfs:/bin/false
usbmux:x:109:46::/home/usbmux:/bin/false
pulse:x:110:116::/var/run/pulse:/bin/false
rtkit:x:111:117::/proc:/bin/false
festival:x:112:29::/home/festival:/bin/false
postgres:x:1000:1000::/home/postgres:/bin/sh
haldaemon:x:113:122:Hardware abstraction layer,,,:/var/run/hald:/bin/false

suninatas:x:1001:1001::/home/suninatas:/bin/sh
```

### [사진 4] 메모장에 옮긴 passwd의 Decoded text

사진 4와같이 Passwd 명의 파일 가장 하단에서 suninatas 계정에 관한 정보를 확인할 수 있었습니다. 리눅스 passwd 파일 시스템의 규칙에 따르면 사용자 이름 다음에 나오는 정보는 암호화된 비밀번호입니다. 이에 x라고 표시되어 있으므로 비밀번호는 암호화되어 shadow에 적혀 있을 것입니다. 따라서 shadow 파일을 확인해보겠습니다.

```
messagebus:x:15426:0:99999:/:
nobody:x:15426:0:99999:7::
mysql:!:15426:0:99999:7::
avahi:*.15426:0:99999:7::
snort:*.15426:0:99999:7::
statd:*.15426:0:99999:7::
usbmux:*.15426:0:99999:7::
pulse:*.15426:0:99999:7::
rtkit:*.15426:0:99999:7::
festival:*.15426:0:99999:7::
postgres:!:15426:0:99999:7::
haldaemon:*.15426:0:99999:7::
suninatas:$6$QlRlqGhj
$BZoS9PuMMRHZZx1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:15427:
0:99999:7::
```

### [사진 5] 메모장에 옮긴 shadow의 Decoded text

사진 5와 같이 Shadow 파일 가장 하단에서도 suninatas 계정에 대한 정보를 확인할 수 있었습니다. 적혀 있는 정보의 형식을 통해 이가 암호화된 비밀번호임을 확인할 수 있습니다.

```
(base) dorothy08ek@localhost:~/forensic$ john password.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
toor (root)
1g 0:00:00:00 100% 1/3 10.00g/s 960.0p/s 960.0c/s 960.0C/s root..r999999
Use the "--show" option to display all of the cracked passwords reliably
Session completed
(base) dorothy08ek@localhost:~/forensic$
(base) dorothy08ek@localhost:~/forensic$ john --show password.txt
root:toor:15426:0:99999:7:::
suninatas:iloveu1:15427:0:99999:7:::
2 password hashes cracked, 0 left
```

#### [사진 6] john 명령어를 통해 확인한 비밀번호

따라서 이를 복호화 하기 위해 복호화 도구를 사용하였습니다.

제가 사용한 도구는 John The Ripper로 해당 파일 전체를 txt 파일로 변환한 후 john [파일명]의 명령어를 통해 해당 문서 파일 내 변환 가능한 암호들을 모두 변환해 주었습니다.

이를 --show 옵션을 사용하여 확인하였습니다.

결론적으로 suninatas 계정의 비밀번호를 확인할 수 있었습니다.

# 5. Flag

iloveu1

## 6. 별도 첨부



## 7. Reference

- [URL]