

작성자	류나연
분석 일자	2024.05.10
작성 일자	2024.05.10
분석 대상	tar파일
문서 버전	01
작성자 E-mail	01star01ek@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부9

7. Reference 10

1. 문제

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

2. 분석 도구

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

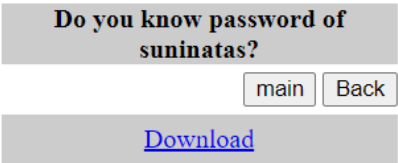
3. 환경

OS
Windows 11, ubuntu 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

Suninatas의 14번 문제는 사진 1번과 같이 password를 찾아 내는 문제입니다.

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

이름	수정된 날짜	유형	크기
오래 전			
shadow	2012-03-28 오전 ...	파일	2KB
passwd	2012-03-28 오전 ...	파일	2KB

[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.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	72	6F	6F	74	3A	78	3A	30	3A	30	3A	72	6F	6F	74	3A	root:x:0:0:root:
00000010	2F	72	6F	6F	74	3A	2F	62	69	6E	2F	62	61	73	68	0A	/root:/bin/bash.
00000020	64	61	65	6D	6F	6E	3A	78	3A	31	3A	31	3A	64	61	65	daemon:x:1:1:dae
00000030	6D	6F	6E	3A	2F	75	73	72	2F	73	62	69	6E	3A	2F	62	mon:/usr/sbin:/b
00000040	69	6E	2F	73	68	0A	62	69	6E	3A	78	3A	32	3A	32	3A	in/sh.bin:x:2:2:
00000050	62	69	6E	3A	2F	62	69	6E	3A	2F	62	69	6E	2F	73	68	bin:/bin:/bin/sh
00000060	0A	73	79	73	3A	78	3A	33	3A	33	3A	73	79	73	3A	2F	.sys:x:3:3:sys:/
00000070	64	65	76	3A	2F	62	69	6E	2F	73	68	0A	73	79	6E	63	dev:/bin/sh.sync
00000080	3A	78	3A	34	3A	36	35	35	33	34	3A	73	79	6E	63	3A	:x:4:65534:sync:
00000090	2F	62	69	6E	3A	2F	62	69	6E	2F	73	79	6E	63	0A	67	/bin:/bin/sync.g
000000A0	61	6D	65	73	3A	78	3A	35	3A	36	30	3A	67	61	6D	65	ames:x:5:60:game
000000B0	73	3A	2F	75	73	72	2F	67	61	6D	65	73	3A	2F	62	69	s:/usr/games:/bi
000000C0	6E	2F	73	68	0A	6D	61	6E	3A	78	3A	36	3A	31	32	3A	n/sh.man:x:6:12:
000000D0	6D	61	6E	3A	2F	76	61	72	2F	63	61	63	68	65	2F	6D	man:/var/cache/m
000000E0	61	6E	3A	2F	62	69	6E	2F	73	68	0A	6C	70	3A	78	3A	an:/bin/sh.lp:x:
000000F0	37	3A	37	3A	6C	70	3A	2F	76	61	72	2F	73	70	6F	6F	7:7:lp:/var/spoo
00000100	6C	2F	6C	70	64	3A	2F	62	69	6E	2F	73	68	0A	6D	61	l/lpd:/bin/sh.ma
00000110	69	6C	3A	78	3A	38	3A	38	3A	6D	61	69	6C	3A	2F	76	il:x:8:8:mail:/v
00000120	61	72	2F	6D	61	69	6C	3A	2F	62	69	6E	2F	73	68	0A	ar/mail:/bin/sh.
00000130	6E	65	77	73	3A	78	3A	39	3A	39	3A	6E	65	77	73	3A	news:x:9:9:news:
00000140	2F	76	61	72	2F	73	70	6F	6F	6C	2F	6E	65	77	73	3A	/var/spool/news:
00000150	2F	62	69	6E	2F	73	68	0A	75	75	63	70	3A	78	3A	31	/bin/sh.uucp:x:1
00000160	30	3A	31	30	3A	75	75	63	70	3A	2F	76	61	72	2F	73	0:10:uucp:/var/s
00000170	70	6F	6F	6C	2F	75	75	63	70	3A	2F	62	69	6E	2F	73	pool/uucp:/bin/s
00000180	68	0A	70	72	6F	78	79	3A	78	3A	31	33	3A	31	33	3A	h.proxy:x:13:13:
00000190	70	72	6F	78	79	3A	2F	62	69	6E	3A	2F	62	69	6E	2F	proxy:/bin:/bin/
000001A0	73	68	0A	77	77	77	2D	64	61	74	61	3A	78	3A	33	33	sh.www-data:x:33
000001B0	3A	33	33	3A	77	77	77	2D	64	61	74	61	3A	2F	76	61	:33:www-data:/va

[사진 3] HxD를 통해 확인한 파일들

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 확인하

[WHS-2] .iso

기 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

Flag 는 iloveu1 으로


(Suninatas – auth 에 입력하면 되었습니다.)





NOTICECHALLENGESAUTHFREETOOLSCHATRANK500Hall Of Fame


Challenges


ALL

WEB

REVERSING

FORENSICS

SYSTEM

MISC

14
199pt / PASS : 1214

15
255pt / PASS : 1408

18
153pt / PASS : 1633

19
154pt / PASS : 1298

21
221pt / PASS : 1107

26
200pt / PASS : 782

28
200pt / PASS : 784

29
266pt / PASS : 346

30
366pt / PASS : 365

31
200pt / PASS : 324

32
180pt / PASS : 346

6. 별도 첨부

7. Reference

- [URL]