

1. 방화벽 로그 분석

ubuntu@ip-172-31-9-64: ~

```
Nov 26 01:17:01 ip-172-31-9-64 CRON[20044]: pam_unix(cron:session): session closed for user root
Nov 26 02:17:01 ip-172-31-9-64 CRON[20115]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 02:17:01 ip-172-31-9-64 CRON[20115]: pam_unix(cron:session): session closed for user root
Nov 26 03:10:01 ip-172-31-9-64 CRON[20180]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 03:10:01 ip-172-31-9-64 CRON[20180]: pam_unix(cron:session): session closed for user root
Nov 26 03:17:01 ip-172-31-9-64 CRON[20190]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 03:17:01 ip-172-31-9-64 CRON[20190]: pam_unix(cron:session): session closed for user root
Nov 26 04:17:01 ip-172-31-9-64 CRON[20264]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 04:17:01 ip-172-31-9-64 CRON[20264]: pam_unix(cron:session): session closed for user root
Nov 26 05:17:01 ip-172-31-9-64 CRON[20345]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 05:17:02 ip-172-31-9-64 CRON[20345]: pam_unix(cron:session): session closed for user root
Nov 26 06:17:01 ip-172-31-9-64 CRON[20488]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 06:17:01 ip-172-31-9-64 CRON[20488]: pam_unix(cron:session): session closed for user root
Nov 26 06:25:01 ip-172-31-9-64 CRON[20502]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 06:25:01 ip-172-31-9-64 CRON[20502]: pam_unix(cron:session): session closed for user root
Nov 26 07:17:01 ip-172-31-9-64 CRON[20629]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 07:17:01 ip-172-31-9-64 CRON[20629]: pam_unix(cron:session): session closed for user root
Nov 26 08:17:01 ip-172-31-9-64 CRON[20700]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 08:17:01 ip-172-31-9-64 CRON[20700]: pam_unix(cron:session): session closed for user root
Nov 26 09:17:01 ip-172-31-9-64 CRON[20771]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 09:17:01 ip-172-31-9-64 CRON[20771]: pam_unix(cron:session): session closed for user root
Nov 26 10:17:01 ip-172-31-9-64 CRON[20843]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 10:17:01 ip-172-31-9-64 CRON[20843]: pam_unix(cron:session): session closed for user root
Nov 26 11:17:01 ip-172-31-9-64 CRON[21284]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 11:17:01 ip-172-31-9-64 CRON[21284]: pam_unix(cron:session): session closed for user root
Nov 26 12:17:01 ip-172-31-9-64 CRON[21365]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 12:17:01 ip-172-31-9-64 CRON[21365]: pam_unix(cron:session): session closed for user root
Nov 26 13:17:01 ip-172-31-9-64 CRON[21437]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 13:17:01 ip-172-31-9-64 CRON[21437]: pam_unix(cron:session): session closed for user root
Nov 26 14:17:01 ip-172-31-9-64 CRON[21508]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 14:17:01 ip-172-31-9-64 CRON[21508]: pam_unix(cron:session): session closed for user root
Nov 26 15:17:01 ip-172-31-9-64 CRON[21583]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 15:17:01 ip-172-31-9-64 CRON[21583]: pam_unix(cron:session): session closed for user root
Nov 26 16:17:01 ip-172-31-9-64 CRON[21655]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 16:17:01 ip-172-31-9-64 CRON[21655]: pam_unix(cron:session): session closed for user root
Nov 26 17:17:01 ip-172-31-9-64 CRON[21762]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 26 17:17:01 ip-172-31-9-64 CRON[21762]: pam_unix(cron:session): session closed for user root
Nov 26 17:32:46 ip-172-31-9-64 sshd[21794]: Accepted publickey for ubuntu from 112.167.182.75 port 24623 ssh2: RSA SHA256:EvSPAhRn4ftTiaL+aAsAMSLpAAhGKngRUmVJUbXhVkwS
Nov 26 17:32:46 ip-172-31-9-64 sshd[21794]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Nov 26 17:32:46 ip-172-31-9-64 systemd: pam_unix(systemd-user:session): session opened for user ubuntu by (uid=0)
Nov 26 17:32:46 ip-172-31-9-64 systemd-logind[488]: New session 215 of user ubuntu.
Nov 26 17:32:50 ip-172-31-9-64 sshd[21794]: pam_unix(sshd:session): session closed for user ubuntu
Nov 26 17:32:50 ip-172-31-9-64 systemd-logind[488]: Session 215 logged out. Waiting for processes to exit.
Nov 26 17:32:50 ip-172-31-9-64 systemd-logind[488]: Removed session 215.
Nov 26 17:33:08 ip-172-31-9-64 sshd[21917]: Accepted publickey for ubuntu from 112.167.182.75 port 24629 ssh2: RSA SHA256:EvSPAhRn4ftTiaL+aAsAMSLpAAhGKngRUmVJUbXhVkwS
Nov 26 17:33:08 ip-172-31-9-64 sshd[21917]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Nov 26 17:33:08 ip-172-31-9-64 systemd-logind[488]: New session 217 of user ubuntu.
Nov 26 17:33:08 ip-172-31-9-64 systemd: pam_unix(systemd-user:session): session opened for user ubuntu by (uid=0)
```

외부에서의 접속 시도가 없었음이 확인된다.

2. AES 암호화 프로그램

사용 라이브러리: PyCryptodome

키: hoduddangkongmom (키우는 강아지와 고양이 이름)

```
1  import base64
2
3  from Cryptodome.Cipher import AES
4  from Cryptodome.Util.Padding import pad, unpad
5
6  password = "hoduddangkongmom".encode('utf8')
7  aes = AES.new(password, AES.MODE_ECB)
8  block_size = 16
9
10 def encrypt(text):
11     byted_text = text.encode("utf8")
12     padded_text = pad(byted_text, block_size)
13     encrypted_text = base64.b64encode(aes.encrypt(padded_text)).decode('utf-8')
14     return encrypted_text
15
16 def decrypt(encrypted_text):
17     decrypted_text = aes.decrypt(base64.b64decode(encrypted_text.encode('utf-8')))
18     unpadded_text = unpad(decrypted_text, block_size)
19     origin_text = unpadded_text.decode('utf-8')
20     return origin_text
21
22 print("1. 암호화 \n2. 복호화")
23 menu = input("메뉴를 선택하세요 ")
24
25 if menu == '1':
26     text = input("문장 : ")
27     encrypted_text = encrypt(text)
28     print("암호화 : ", encrypted_text)
29
30 elif menu == '2':
31     text = input("문장 : ")
32     decrypted_text = decrypt(text)
33     print("복호화 : ", decrypted_text)
34
35 else: print("올바르지 않은 메뉴입니다.")
```

실행 예

```
1. 암호화
2. 복호화
메뉴를 선택하세요 1
문장 : my cat is cute
암호화 : dcxmoVTuxCGcXUMUF3D7Yg==
```

```
1. 암호화
2. 복호화
메뉴를 선택하세요 2
문장 : dcxmoVTuxCGcXUMUF3D7Yg==
복호화 : my cat is cute
```

3. 해시를 이용한 파일 변조 확인

실행 예 1

분석한 파일의 MD5

Windows embeddable package (32-bit)	Windows		0888959642cc8af087d88da3866490a5	9560053	SIG	CRT	SIG
-------------------------------------	---------	--	----------------------------------	---------	---------------------	---------------------	---------------------

계산한 MD5

```
1 import hashlib
2
3 def MD5_hash(path):
4     f = open(path, 'rb')
5     data = f.read()
6     hash = hashlib.md5(data).hexdigest()
7     return hash
8
9
10 file_name = input("파일 이름을 넣으세요. ")
11 hash_value = MD5_hash(file_name)
12 print("파일의 해시 값(md5)은 ", hash_value)
```

PROBLEMS 4 OUTPUT DEBUG CONSOLE TERMINAL

TERMINAL Python Debug Console +

파일 이름을 넣으세요. python-3.11.0-embed-win32.zip
파일의 해시 값(md5)은 0888959642cc8af087d88da3866490a5

실행 예 2

분석한 파일의 MD5

Windows installer (64-bit)	Windows	Recommended	4fe11b2b0bb0c744cf74aff537f7cd7f	25157416	SIG	CRT	SIG
----------------------------	---------	-------------	----------------------------------	----------	---------------------	---------------------	---------------------

계산한 MD5

```
1 import hashlib
2
3 def MD5_hash(path):
4     f = open(path, 'rb')
5     data = f.read()
6     hash = hashlib.md5(data).hexdigest()
7     return hash
8
9
10 file_name = input("파일 이름을 넣으세요. ")
11 hash_value = MD5_hash(file_name)
12 print("파일의 해시 값(md5)은 ", hash_value)
```

PROBLEMS 4 OUTPUT DEBUG CONSOLE TERMINAL

TERMINAL Python Debug Console +

파일 이름을 넣으세요. python-3.11.0-amd64.exe
파일의 해시 값(md5)은 4fe11b2b0bb0c744cf74aff537f7cd7f