node1 靶机渗透指南

156****3330 / 2018-10-16 22:07:25 / 浏览数 2661 安全技术 CTF 顶(1) 踩(0)

---

node1 靶机渗透指南

靶机下载地址和环境

靶机下载地址:https://download.vulnhub.com/node/Node.ova

靶机的环境:处于nat网络的vm虚拟机中

实战

首先知道靶机的Ip地址

这里提供两种办法给大家

第一种是使用 `arp-scan -l` 获取局域网内其他主机

第二种是使用 `nmap 192.168.138.0/24`扫描

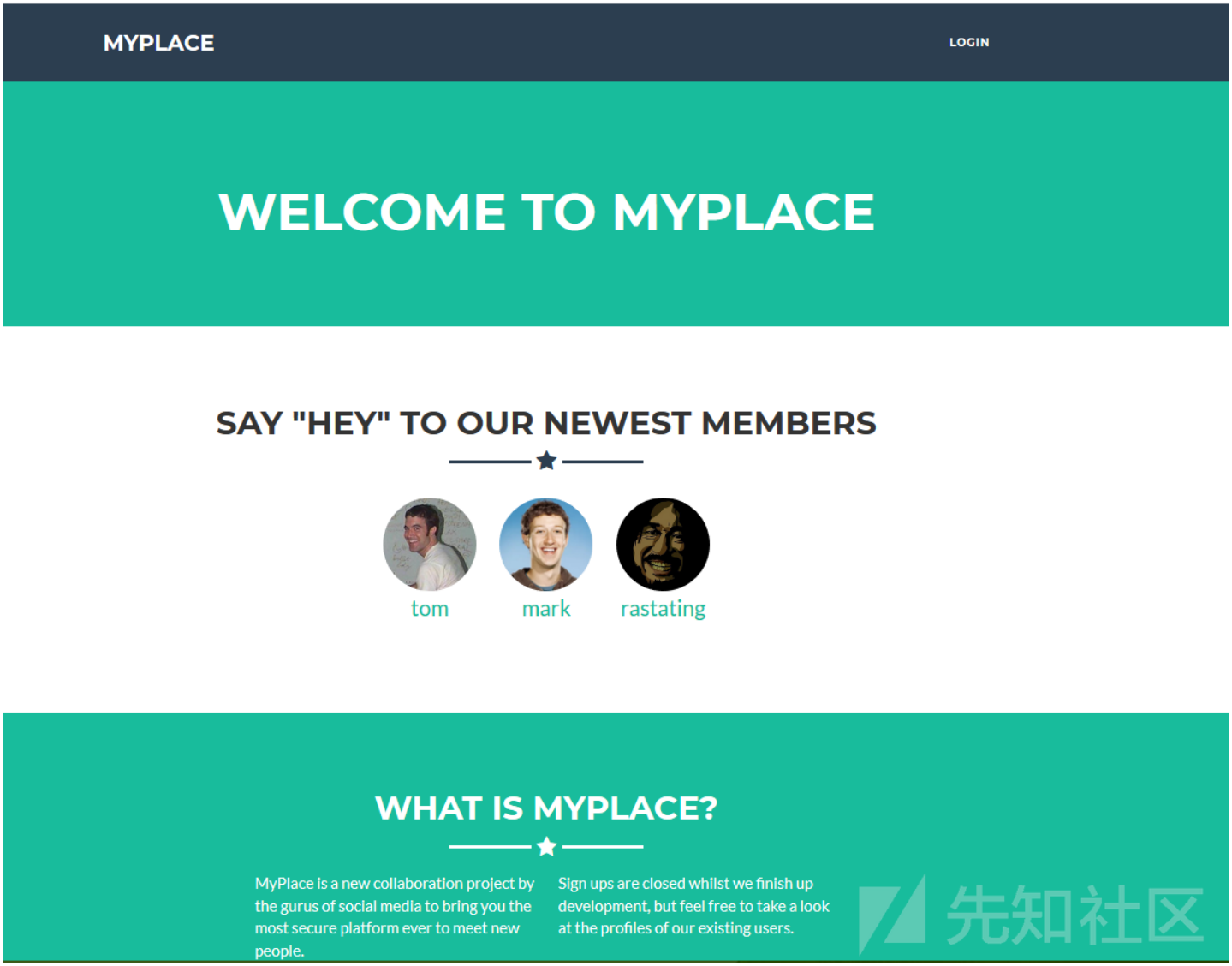
最后得到我们的目标主机的ip地址是 `192.168.138.137`

按照惯例我们使用`nmap -A 192.168.138.137` 获取详细信息

扫描结果发现目标开启了 22 ssh端口 和 3000端口

对node.js稍有了解的都知道 3000是node.js的默认端口

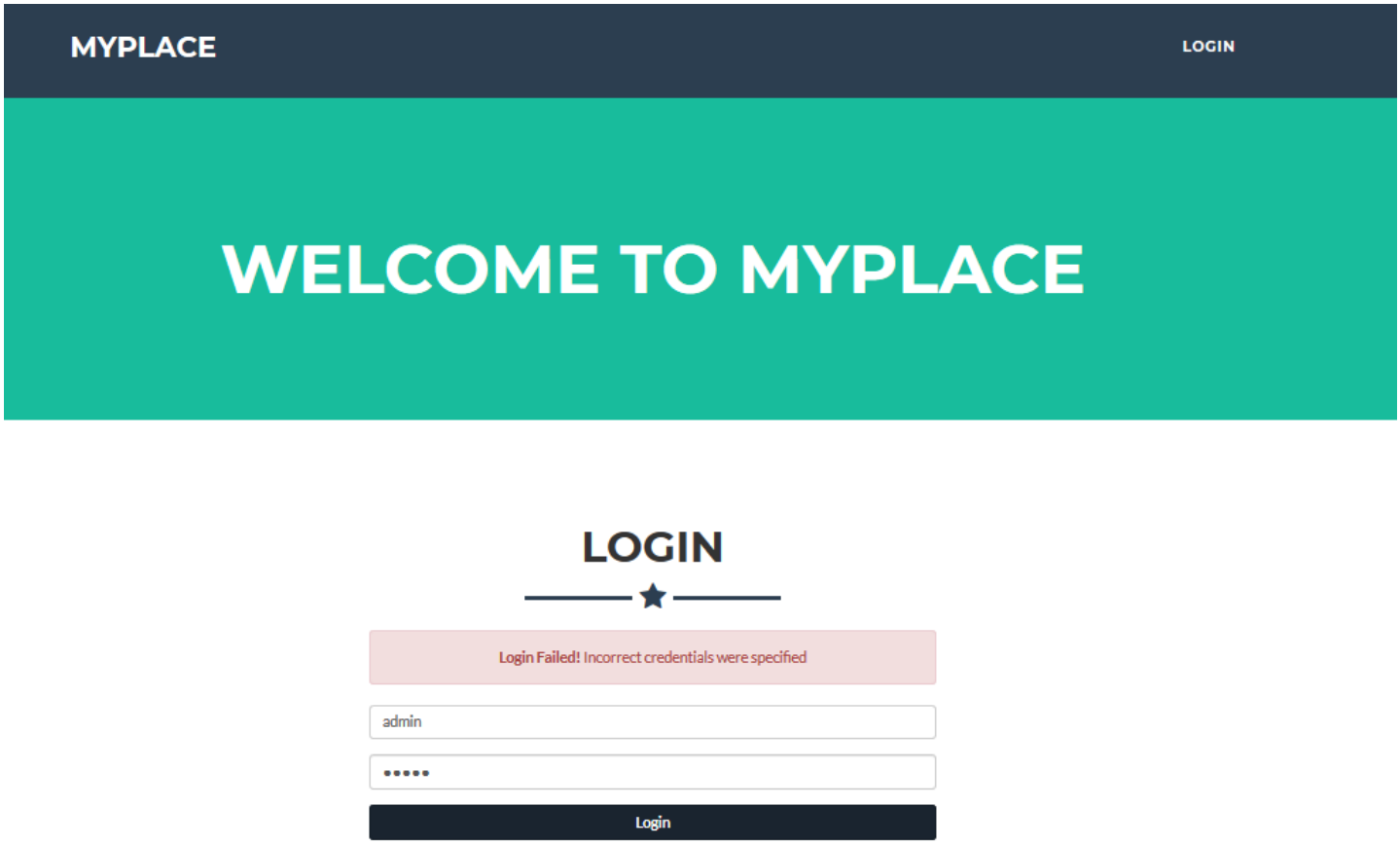
访问`192.168.138.137:3000`



欢迎界面如上

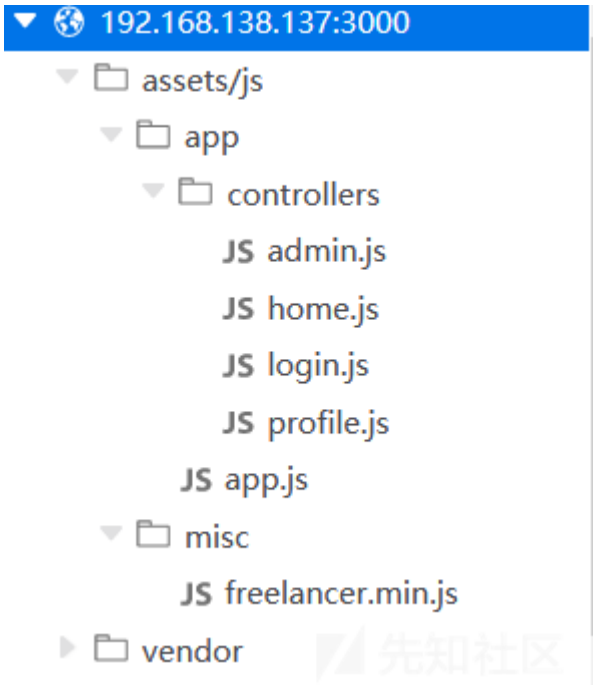
发现右上角的 LOGIN 蛮惹眼de

于是乎 尝试 `admin admin`



结果当然是想当然

继续打开控制带看一下



发现这个网站的 js 文件命名有点意思

于是逐一审计 发现了一些可疑路劲

尝试访问`http://192.168.138.137:3000/api/users/latest`后得到以下信息

JSON 原始数据 头

保存 复制 全部折叠 全部展开


```
0:
    _id:        "59a7368398aa325cc03ee51d"
    username:   "tom"
    password:   "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240"
    is_admin:   false
1:
    _id:        "59a7368e98aa325cc03ee51e"
    username:   "mark"
    password:   "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73"
    is_admin:   false
2:
    _id:        "59aa9781cced6f1d1490fce9"
    username:   "rastating"
    password:   "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0"
    is_admin:   false
```


这岂不是把账户密码爆出来了呀 只不过密码是经过加密的

这是看到最后的 `latest`有点意思 不如把它去掉

再次访问 发现得到了一个管理员用户

JSON 原始数据 头

保存 复制 全部折叠 全部展开


```
0:
    _id:        "59a7365b98aa325cc03ee51c"
    username:   "myP14ceAdm1nAcc0uNT"
    password:   "dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af"
    is_admin:   true
1:
    _id:        "59a7368398aa325cc03ee51d"
    username:   "tom"
    password:   "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240"
    is_admin:   false
2:
    _id:        "59a7368e98aa325cc03ee51e"
    username:   "mark"
    password:   "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73"
    is_admin:   false
3:
    _id:        "59aa9781cced6f1d1490fce9"
    username:   "rastating"
    password:   "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0"
    is_admin:   false
```

而首先我们要破解密码 可以使用kali虚拟机自带的工具
`hash-identifer` 来识别

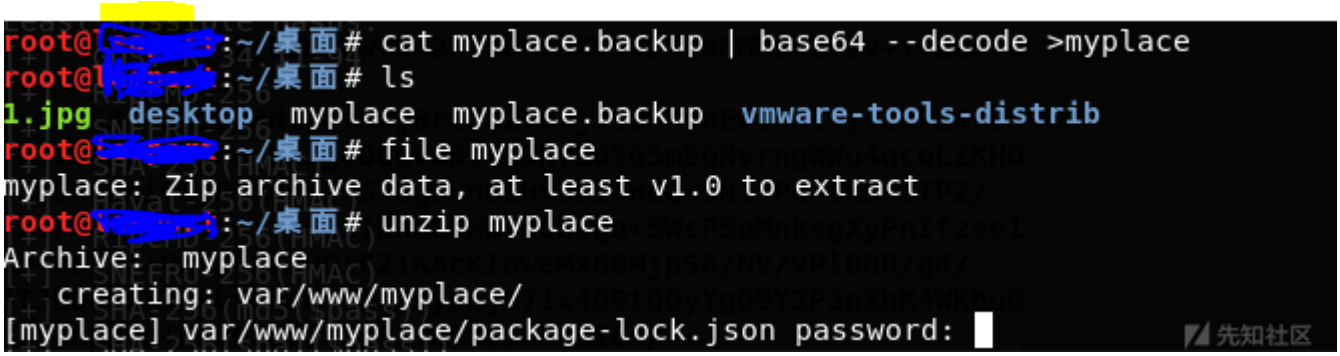
最后再使用一个在线的解密网站

http://md5decrypt.net/

得到密码是 `manchester`

登录后发现 可以下载网站备份

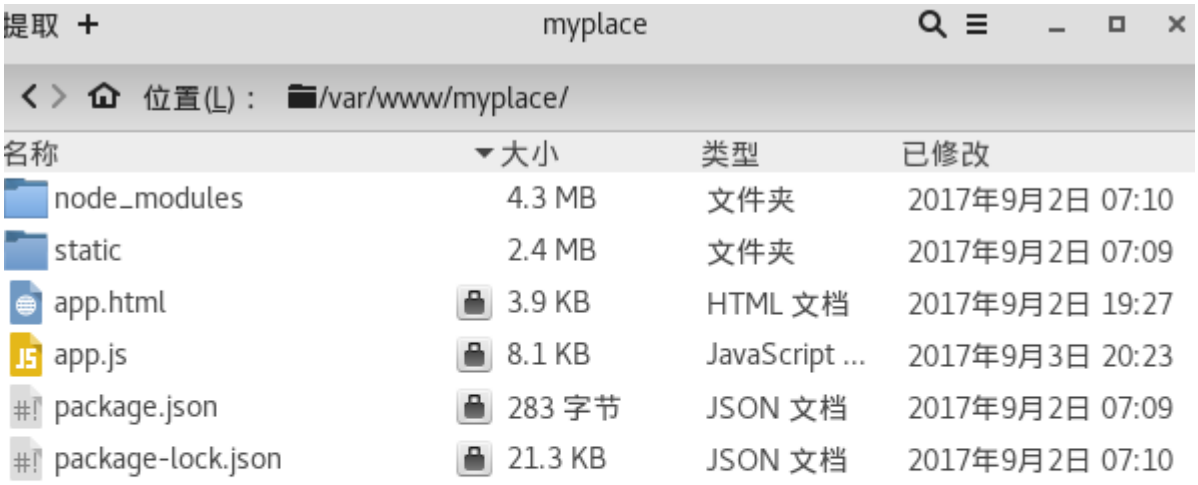
尝试以base64解码后压缩包打开 提示需要密码



这个时候我们可以使用kali自带的工具
`fcrackzip`进行破解

通过字典猜解出密码为magicword

打开后如图这是网站的目录



对于node.js而言我们首先要基本熟悉他的构架

https://www.cnblogs.com/Chen-xy/p/4466351.html

其中 app.js：项目入口及程序启动文件。

那我们先从这里开始

```
const express     = require('express');
const session     = require('express-session');
const bodyParser  = require('body-parser');
const crypto      = require('crypto');
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const path        = require("path");
const spawn        = require('child_process').spawn;
const app         = express();
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
const backup_key  = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';
```

这里发现了一个Node.js 连接 MongoDB 的操作

Node.js连接MongoDB

这个mongodb实例指向localhost，所以很可能这些凭证也适合ssh访问

尝试一波

```
ssh mark@192.168.138.137
```

成功登录 查看系统信息


```
mark@node:~$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

接下来是提权操作

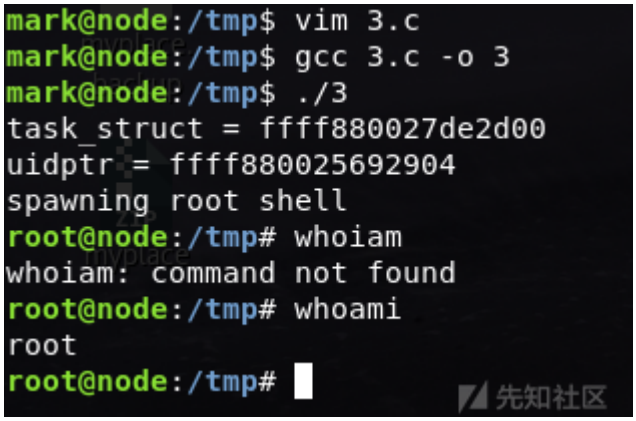
我们可以使用`searchspolit` 查找漏洞或者网上找下 exp

如图 那我们就开始利用吧

用scp命令 scp■ secure copy■■■, scp■linux■■■■■ssh■■■■■■■■■■■■■■■■
把我们的exp上传到靶机

这里我们采用 [Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation]

把代码copy到tmp文件下然后编译执行即可



点击收藏 | 3 关注 | 1

上一篇：护网杯2018 easy_lara... 下一篇：ethernaut 题目Alien...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板