【探讨】一次不算太成功的渗透

hades / 2017-12-29 11:00:17 / 浏览数 5618 安全技术 技术讨论 顶(1) 踩(0)

先整体说说目标的一个整体概况吧，此目标站点5年之前搞下过它的另外一台服务器，主服务器一直没有搞定，所以这次继续上次没完成的任务，go on 欢迎各位师傅探讨探讨各种姿势

目标站点：

1. 单独服务器——美国加利福尼亚州洛杉矶 hostspaces
2. 在线扫描了一下服务器大体端口开放情况如下，和实际效果应该有点偏差，后续再扫描

```
Starting Nmap ( http://nmap.org ) at 2017-12-27 18:17 EET
NSE: Loaded 29 scripts for scanning.
Initiating SYN Stealth Scan at 18:18
Scanning www.ro***.com (*.*.*.*) [100 ports]
Discovered open port 3306/tcp on *.*.*.*
Discovered open port 80/tcp on *.*.*.*
Discovered open port 22/tcp on *.*.*.*
Discovered open port 21/tcp on *.*.*.*
Discovered open port 9999/tcp on *.*.*.*
Completed SYN Stealth Scan at 18:18, 1.99s elapsed (100 total ports)
Initiating Service scan at 18:18
Scanning 5 services on www.ro***.com (*.*.*.*)
Completed Service scan at 18:18, 6.30s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.ro***.com (*.*.*.*)
Retrying OS detection (try #2) against www.ro***.com (*.*.*.*)
Initiating Traceroute at 18:18
Completed Traceroute at 18:18, 2.13s elapsed
NSE: Script scanning *.*.*.*

[+] Nmap scan report for www.ro***.com (*.*.*.*)
Host is up (0.15s latency).
Not shown: 90 closed ports

PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
22/tcp   open     ssh          OpenSSH 5.3 (protocol 2.0)
80/tcp   open     http         nginx      Scan with Web Server Scanner
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1025/tcp filtered NFS-or-IIS
3306/tcp open     mysql        MySQL (unauthorized)
5357/tcp filtered wsdapi
9999/tcp open     http         nginx      Scan with Web Server Scanner

Aggressive OS guesses: Linux 3.1 (91%), Linux 3.2 (91%), Linux 2.6.23 - 2.6.38 (91%), Lexmark X644e printer (91%), AXIS 210A o
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
1025/tcp filtered NFS-or-IIS
3306/tcp open     mysql
4444/tcp filtered krb524
5555/tcp open     freeciv
6129/tcp filtered unknown
9999/tcp open     abyss
```

80端口

运行的一套阉割版本的DeDe系统，很多文件都已经删除，只保留了基本的显示功能，通过以前的数据登录会员系统，发现只有一个充值的功能what fuck？

我一度的怀疑这个网站没有管理后台，那站长每天的更新是如何实现的？？？？或者是用的其他域名来作为管理后台的，我社工进入了管理员的51la统计系统，在每天的来源

9999端口

主机宝linux版本，暂时没有0day无果，找朋友分析源代码中

社工

由于以前搞过一次，所以回忆一下以前的过程，目标站以前交易的时候还是支付宝，留意的一下支付宝的名称，当时kuzi还比较流行，用昵称和各种收集到的信息去茫茫数据

邮箱

时间太过久远，估计上次也被站长发现了，所以站长修改了密码，当时的网易邮箱还是可以通过密保问题找回密码的，站长虽然修改了密码，但是密保的问题答案还是原邮箱

最近继续渗透的时候，发现找回密码都是用手机了，没有其他方式找回。。。。在原有的信息当中寻找突破，突然人品爆测试了几次直接杀进去了。

看来还是支付宝关联的账号使用频率还是挺高的，，，每天都有交易

Ps：登录邮箱的时候注意邮箱的风控策，朋友当时想用客户端关联邮箱接收邮件，关联完成后，邮箱立马来了一份异常报警邮件，由于我知道站长的活动地域，我直接用手机

上一篇：分享一个二进制文件上传技巧 下一篇：Pentest Wiki Part...

1. 16 条回复

evil7 2017-12-29 11:03:32

2017年没做完的事就要在2018年来之前解决，支持往死搞

0 回复Ta

castiel 2017-12-29 11:12:41

扫下二级域名看能不能有所收获 或者是找到管理地址。
社下域名信息看是哪家idc 看能不能控制域名
搜集管理日常信息 个人习惯，嗜好，发邮件钓鱼

0 回复Ta


ftkahzmodan 2017-12-29 11:18:10

不要跟我讲什么社工0day，渗透就是一把梭！拿着啊D就是干！

2 回复Ta


hades 2017-12-29 11:29:08

@ftkahzmodan o(￣ ▽ ￣)o呵呵

0 回复Ta


hades 2017-12-29 12:26:36

@castiel pdns数据过了一部分 没有找到其他二级域名 后续再更新

0 回复Ta


wooyun 2017-12-29 13:07:01

冰总明目张胆黑网站，收徒不

0 回复Ta


wing 2017-12-29 14:55:40

@wooyun hades是冰总？

0 回复Ta


hades 2017-12-29 15:12:00

@wing 嗯 是我

0 回复Ta


sofia 2017-12-29 16:04:01

楼主会不会刷钻

0 回复Ta


farmsec 2017-12-29 16:32:42

看他使用的密码规则。以及个人信息。再生成一份新的字典。去跑其他，比如ftp ssh mysql 。
然后查看这个邮箱/手机号注册的其他邮箱网站。还有他媳妇的，寻找更多的突破口。或者直接给他带个帽子~~~

0 回复Ta


answer 2018-01-02 10:28:53

我觉得 最好的就是挖掘一个主机宝的0day了，直接一把梭

0 回复Ta


ssss 2018-01-02 14:52:00

还是这种文章看起来有意思qwq

0 回复Ta


saint 2018-01-03 16:16:13

冰总再次出山了！

0 回复Ta


helentadie 2018-02-09 20:54:42

看到通过密保修改密码，冰总手里有裤子啊。。。

0 回复Ta


hades 2018-03-08 18:05:26

@helentadie 没有 是当时社工站长收集到的一些信息，各种组合测试。。那叫一个心酸啊。。

0 回复Ta


master 2018-03-27 17:56:36

@hades 我大概能猜到哪个站，rois还是什么来着，以前经常说这个站，是吧

0 回复Ta

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