APT之迂回渗透

关于我

Id：小越（旭日）

Form：08sec

Focus on：

Twitter：

目录

引言

一 信息收集

二 漏洞利用

三 横向渗透

四 内网渗透

总结

引言

随着信息安全行业发展，很多企业，政府以及互联网公司对网络安全越来越重视。习大大指出，没有网络安全就没有国家安全，没有信息化就没有现代化。

众所周知，现在的安全产品和设备以及对网络安全的重视，让我们用常规手段对目标渗透测试的成功率大大降低。当然，对于一些手握0day的团队或者个人来说，成功率还是很高的。

迂回渗透：迂回，是指在思想或表达方式上绕圈子的性质或状态；从字面上讲是曲折回旋的；环绕的。迂回曲折。渗透，指渗入;透过液体渗透多孔物体。另还比喻某种事物或势力逐渐进入其他方面。这里所说的意思是避过正面安全产品和设备，从“侧面”进行渗透。这个“侧面”就是我们现在一起交流的一个方式

信息收集

目标是某特殊机构，外网结构简单，防护严密。经探测发现其多个子机构由一家网站建设公司建设。

对子域名进行挖掘，确定目标ip分布范围及主要出口ip。

很多网站主站的访问量会比较大。往往主站都是挂了CDN的，但是分站就不一定了，所以可能一些分站就没有挂CDN，所以有时候可以尝试通过查看分站IP，可能是同个IP或者同个站。shodan.io ,fofa.so、

MX 及 邮件。mx记录查询，一般会是c段。

一些网提供注册服务，可能会验证邮件。

还有RSS订阅邮件、忘记密码、利用crossdomain.xml的跨域设置特性，域传送漏洞等。

也可以通过ssl证书进行域名探测，使用censys.io判断是机房还是公司机构

真人 公司ip归属段。
通过公网判断目标是否存在内网。我个人认为这个比较重要

censys

Certificates defcon.org

Sign In

Results Report Docs

Quick Filters

For all fields, see Data Definitions

Tag:

- 34 CT
- 34 Google CT
- 34 Leaf
- 19 Expired
- 19 Previously Trusted

More

Issuer:

- 26 DigiCert Inc
- 5 Trustwave Holdings, Inc.
- 2 Network Solutions L.L.C.
- 1 COMODO CA Limited

Certificates

Page: 1/2 Results: 34 Time: 709ms

C=US, ST=Washington, L=Seattle, O=DEF CON Communications, Inc., CN=p2p-s0.defcon.org

DigiCert SHA2 Secure Server CA
2019-01-19 – 2021-02-02
databank.defcon.org, p2p-s0.defcon.org, p2p-s1.defcon.org, p2p-s2.defcon.org, ...
parsed.names: databank.defcon.org

C=US, ST=Washington, L=Seattle, O=DEF CON Communications, Inc., CN=p2p-s0.defcon.org

DigiCert SHA2 Secure Server CA
2019-01-19 – 2021-02-02
databank.defcon.org, p2p-s0.defcon.org, p2p-s1.defcon.org, p2p-s2.defcon.org, ...
parsed.names: p2p-s1.defcon.org

businessCategory=Private Organization, jurisdictionCountry=US, jurisdictionStateOrProvince=Washington, serialNumber=601960672, street=406, street=2606 2nd Ave, postalCode=98121, C=US, ST=Washington, L=Seattle, O=DEF CON Communications, Inc., CN=www.defcon.org

DigiCert SHA2 Extended Validation Server CA
2017-05-26 – 2019-05-31
defcon.org, forum.defcon.org, media.defcon.org, www.defcon.org, ...
parsed.extensions.subject_alt_name.dns_names: www.defcon.org

漏洞利用

在此说明一下，不方便截图，今天我来和大家分享一下这个渗透思路。这个公司供应商，我们要搞的是供应商的其中一个客户。

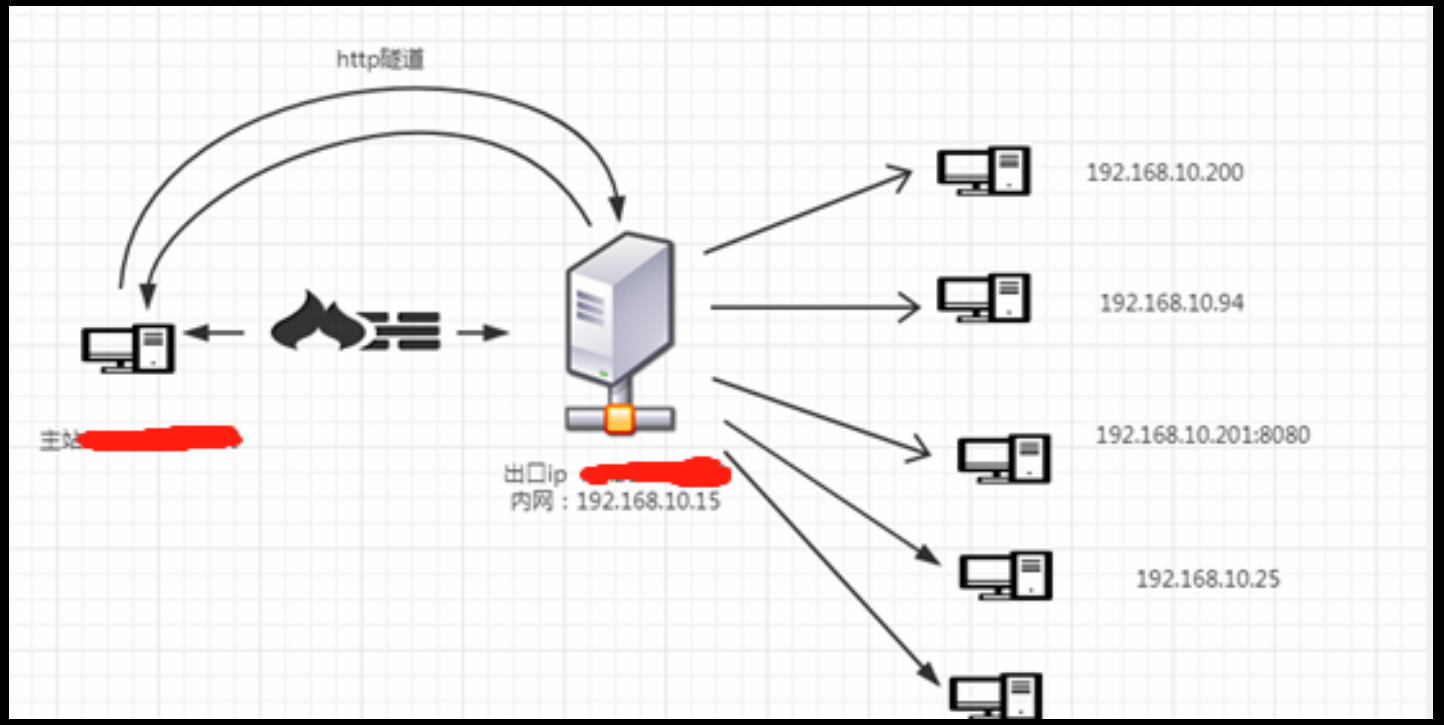
对子域名进行模糊探测，可以使用常见扫描器进行轻扫描。确定其服务器类型，使用脚本类型，常用cms。

发现一个文件包含，通过phpinfo获取网站跟目录及ip，经过检测发现该系统有任意文件读取漏洞。利用这个漏洞获取linux常见配置文件，web数据库配置文件。通过读取各类配置文件密码组合生成字典，爆破主站管理、ssh、FTP及找到的各种登陆口，从FTP上传php脚本目标，拿到shell。

横向渗透

先确定获取的服务器所在网络位置有无内网，从数据区读取管理员账号密码，其他配置文件及备份文件，发现xxip登陆频繁。（拿到shell第一时间是信息获取）

该ip处于子域名另外一个网段，通过主站做代理，登录xxip机器，该主机有存在内网ip，处于内网边界处。



代理：绕过防火墙及包过滤、协议过滤防火墙

做代理及端口转发几个方式：
系统自带，ssh iptables netsh
第三方: lcx ht socks phpsocks metasploit reg ew
在找到内网入口注意几点：

1 不要第一时间进行深入
2 要第一时间巩固入口权限
3 获取和分析这台机器的数据和在网络中的作用
4 分析管理员的登录习惯，避免与管理员同时操作
5 制定下一步的工作目标。
6 开始做代理通道进行横向扩展。（能不做代理就不要做代理）

通过代理，本地打开邮件服务器管理登陆，管理所有通讯邮件，备份出邮件服务器数据，本地恢复分析出该公司与客户的通讯信息。

内网渗透

在内网机器中搜索信息进行横向移动，组合字典爆破内网机器。在内网机器上翻阅相关文件及以控制数据库中可能存储配置口令（别忘了回收站），服务器当前所在网段的所有主机端口，服务器ARP缓存，服务器上的服务，内网中其他HTTP服务。

下载mstsc文件，查看登录记录。通过cmdkey /list 查看本地保存的登录凭证。

内网渗透：

1 想要获取的目标信息：邮件服务器，文件服务器，人员数据。
2 关键用户凭证：域管，it管理员，默认管理账号。
3 关键计算机：连接各个网段的机器。
4 内网机器后门：域管，it管理员等管理账号经常登录的机器。

域渗透：

1 获取域信息（域管，邮件服务器，文件服务器）。
2 尝试抓取域管账号密码。
3 利用普通域用户提权到域管理员。
4 利用ms17010永恒之蓝获取用户帐户密码。
5 导出域hash，为以后再次进入做准备。
6 尝试找出该机构vpn账号密码和登录口。

工作组渗透：

1 尽可能获取机器的默认管理账号密码。
2 利用ms17010永恒之蓝获取用户帐户密码。
3 尝试找出该机构vpn账号密码和登录口。

补充：

内网再次准备：上远控，找vpn，出口webshell。

通过内网渗透控制该公司，掌握与该公司目标客户通讯渠道，邮件等。

权限维持：

1.通过数据流建立隐藏webshell，设置权限防改防删，端口复用
建立万能后门（iis apache tomcat）
2.dns/icmp/http远控，对windows/linux权限维持，windows马无进程无端口
3.挖掘源码漏洞，修改源码及备份文件加入已知后门或建立有漏洞文件，并建立不死文件
4.域渗透金钥匙，控制域内机器
5.msf persistence/metsvc模块
6.powershell脚本

进入目标客户的方式：

1 通过系统更新渠道推送马
2 通过客户登陆的WEB服务页面定向挂马（过滤来源IP）
3 通过管理页面挂马，马的使用 炮灰马 大量撒网挂马， 长期控制隐蔽马
4 远程维护，很多企业要给客户开内网权限进行系统维护
5 代码审计发现系统通杀漏洞

由于我们这次的目标是迂回渗透，对该公司的资料不感兴趣。如果要是需要大量文件（5g以上）就需要文件回传。（例如科技公司的研发文件服务器）。
文件处理

1 文件筛选：把文件的目录树取回来，分析需要的文件目录。
2 文件回传：文件分卷加密压缩，多台内网机器进行ipc多层中转，本地组建拖文件集群，每个IP回传一定大小文件，哈希校验，边传边删，本地解压重建。

日志清理：
由于我的习惯，我操作的我自己清理，大部分都是文件，简单的清理，动作也不大。估计是我对自己有信心二次进入吧。

总结

内网渗透注意事项：

- 扫描
- 远程登录
- 爆破
- 溢出提权

能手工尽量不用工具，能不使用交互模式尽量不用交互，能不上传文件尽量不要上传，能一把菜刀cmd命令行下解决的就不要用其他的。

谢谢大家!