

畅谈端口安全配置—安全小课堂第十四期

京东安全应急响应中心 2016-06-17

安全小课堂第十四期

众所周知，计算机之间通信是通过端口进行的。黑客常常利用这些端口来实施入侵，因此掌握端口的安全配置知识，是安全上网必备的技能。本期我们来聊一聊端口安全的配置。

本期邀请到了来自万达电商安全专家rootsecurity、唯品会安全专家池中物，还有京东安全负责端口的小伙伴一起参与讨论哟~

1



豌豆妹

配置端口安全时，应当注意哪几类问题呢？



哆啦A梦

1. 端口白名单默认只开通80，443，其他端口不要往外放，避免不必要的安全风险。
2. IDC流量默认只进不出，防止端口反弹。如要开通出向流量，需提流程申请。
3. 可能有人会问，不让上网，我如何安装软件？这个就需要自己发挥智商了，如果有资源就自己搭建yum源，如果没有资源最笨的办法就自己打通用的rpm包。
4. 之前渗透的场景遇到过把类似于ftp（默认：21）ssh（默认：22）改成别的端口以躲避扫描的，例如211.149.160.80这个ip，就把3389，改成33890了。这里我想特别强调下这个问题，改端口是避免不了被黑的，只不过是看黑你的人有没有耐心对付你，这种情形，要么你就加白名单，要么就不要对外开放，当然我还是建议外部不要开放类似这些服务，会增加安全隐患。



我从端口安全策略上说说自己的一些看法。个人认为配置端口安全策略需要注意的问题有以下几点：

1. 应贴紧业务。因为端口安全策略的需求往往是业务方提出的，只有充分了解业务的需求才能确定端口的访问是否有足够的安全。
2. 端口安全标准化。标准化后的业务才能大大减轻运维和网络等部门的工作量。
3. 端口安全的支撑是访问控制策略框架。有了框架只需将业务需求进行合耦就能制定出标准。
4. 合规性，pci，银行支付等等都会对端口访问控制有要求。
5. 持续改进，失效策略等的问题。

2



豌豆妹

那能介绍下实现端口安全的几种机制么？也就是平时如何配置安全端口。



小丸子

实现端口安全的机制有：

1. 端口应按安全性来进行分类，如：web类，app类，传输类，通信类，加密类等。
2. 区域安全性分类，如高密区、中密区、低密区、中转区、DMZ等
3. 制定通用端口，通用端口往往是业务量最大的策略，而且安全性比较高的。
4. 外网端口监控，定时监控、告警和响应。
5. 网络信息库收集，包括ip管理。
6. 安全策略集中管理，如使用“管理系统”实现。



小新

1. 我们目前所有非 80 , 443 的端口对外开放时应加白名单 , 不允许 **permit any any** (思科设备的命令 , 就是允许所有的操作) 的操作。
2. 如果服务本身有授权功能的 , 必须要开启授权功能 , 比如 **mongodb , redis** 这些。
3. 对外开放的服务 , 例如 redis , mongodb , snmp , ntp 这些服务都是近些年出现安全攻击的弱点。很多姿势这里就不一一列举了 , 比如 snmp 服务如果配置有问题可能会用 **public** 读取路由器的配置 , 进而获取 console 的密码登录设备 , 甚至登录 VPN 漫游内网。还有去年 11 月爆发的 redis 未授权访问服务 , 1 周之内几乎全球的可以匿名登录的 redis 都被写入了 **crackit** 的这么一个 key。但 redis 这个问题肉鸡上线率还是很高的。
4. 最后来说一下如何安全配置这些服务 , 像 redis , mongodb 这些服务能启用 authorization 的就启用 , 给攻击者增加攻击成本。同时保护自己。另外像 snmp , ntp 这些服务务必要加白名单 , **只允许可信设备读取** , 其他的一律拒绝。

3



豌豆妹

若业务要求开放不安全端口 , 如何去配置呢 ?



哆啦A梦

1. 变更部署方式 , 如端口是不安全的 , 可以将业务部署到相对安全的区域里面 , 或在一个隔离的状态里面访问。
2. 变更端口使用方式 , 如端口是 telnet 等不安全的端口访问 , 需要变更为 ssh 等加密方式。
3. 增加应用层防护 , 如 rsync 文件同步 , 可在 **配置文件里限制访问的源 ip** , 也就是白名单方式 , **ntp 的访问有放大攻击的危险** , 可升级相关版本和配置禁止远程修改等配置。
4. 安全检查 , 对于不安全的一些业务端口请求 , 需要对业务系统的安全性进行测试或检查 , 其中包括主机服务器基线安全等 , 通过后才能开放。
5. **对外网的访问 , 高危端口一律不开放** , 如 : ssh、1433、3306 和 telnet 等等。



葫芦娃

这个分两方面来看：

第一：如果公司安全部门之前制定过相关规定，那就直接按照规定执行。

第二：如果之前没有类似的规定而业务又必须开放的这种情形一定要把该机器物理隔离，尽量降低出现风险带来的安全隐患，如果有条件尽量使用虚拟化去解决他（她）的业务需求，同时安全部门要介入将外开放的端口进行安全加固。

小新



给大家举个栗子。

危害举例：

<http://www.wooyun.org/bugs/wooyun-2010-0198472>；

<http://www.wooyun.org/bugs/wooyun-2010-052749>。



豌豆妹

变更部署方式能具体说下吗？

葫芦娃



就是增加中间区域或变更成统一安全等级的区域来进行访问。我们这里的环境是有一个叫中转区，进入中转区的服务器或设备要经过安全检查的，就是从网络安全区域上限制。

4



豌豆妹

如何监控公司端口？是只扫描常用端口，还是全部端口？

哆啦A梦



这两种情形我认为都需要监控，常用端口每天一报，全部端口每周一报。如果有异常端口对外开放，必须及时处理。

葫芦娃



使用端口扫描工具将相关的结果加入到soc中实现监控、告警和响应。当然这里还要对端口的安全性进行定义，定义一些高危端口。

5



豌豆妹

监控端口的扫描工具有哪些呢？

小丸子



我比较常用的工具有nmap，可以自己写脚本批量扫，当然，除了nmap之外，还有一个改进版的工具是由WooYun白帽子猪猪侠基于libnmap写的一款端口扫描和服务指纹识别的程序，传送门：[\[http://github.com/ring04h/wyportmap.git\]](http://github.com/ring04h/wyportmap.git)同时，如果该服务需要破解的话可以基于hydra或者medusa去爆破，如果RP不错的话，还是有一定成功率的。另外常用端口的范围还是需要自己去定义的。

葫芦娃



扫描端口验证：nmap。

端口弱口令验证工具：hydra、ncrack。

端口反弹：rtcp.py脚本、多平台网络穿透工具EW。



豌豆妹

扫描的端口也是自定义的吗？



哆啦A梦

恩，nmap有个参数是 `—open -p` 检测开放端口的。比如全部扫描可以使用 `—open -p1-65535`，略慢。



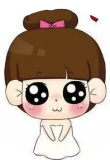
豌豆妹

有一些扫描出的非常规端口，也不知道开启的是什么服务。这个怎么去判断呢？



哆啦A梦

这个服务指纹识别是一个很大的项目，主要是基于 **banner** 去判断。比如是ssh服务，可以写正则 `'ssh|^SSH-'` 或 `'ssh|^SSH-.*openssh'` 之类的。banner只要返回这些，正则匹配上，就可以证明是ssh服务。



豌豆妹

可是有时候一些返回的是空的。类似于这种。

```
tcp      | 9209 |      | open |
tcp      | 9250 |      | open |
tcp      | 9319 |      | open |
tcp      | 9320 |      | open |
tcp      | 9321 |      | open |
```

哆啦A梦



返回是空，这就要靠手工判断了。

葫芦娃



我也发现有些端口是空返回，这种有一部分是建立了tcp三次握手，但后面没有挂载服务，返回空的。除了tcp，其实udp的连接也需要关注，因为udp的很容易就可以伪造。

哆啦A梦



补充一点。还有一种情况就是，防火墙建立三次握手的时候会告诉你，我1-65535端口都是开放的，这种情况和环境比较恶心。其实该端口下，并没有什么服务。这种情况其实有很多，我们发现一般都会进行过滤的。



豌豆妹

方便透漏下你们nmap的参数吗？

小丸子



这个需求不同，参数不一样，可以参考猪猪侠那个项目里的参数`global_options = '-sT -P0 -sV -O --script=banner -p T: port'`。我手动的时候经常 `--open -p1-65535`。

小新



是的，一般会是65535的，再加上udp的一些端口。123、161、53、5060、等等。

6



豌豆妹

对于端口监控，有什么比较好的办法让程序完全自动化？

葫芦娃



我们使用的是soc，增加高危端口的索引，就是发现后可以发邮件、预警短信等。针对外网是高危端口。内网我们有相关的运维制度，因为端口的开放往往和运维相关。比如web应用我们会有相关的端口范围，如果想访问必须走oa申请和变更流程。按现在互联网公司的发展看，端口问题出现最多的是在一些创新业务，因为创新业务上面对端口的界定我们要进行安全评估才能做相关的申请，会比一般的严格。



豌豆妹


哇哈~又学到了新知识~开心!!!感谢大家的关注哟~

安全小课堂往期回顾：

- 1、论安全响应中心的初衷；
- 2、安全应急响应中心之威胁情报探索；
- 3、论安全漏洞响应机制扩展；
- 4、企业级未授权访问漏洞防御实践；
- 5、浅谈企业SQL注入漏洞的危害与防御；
- 6、信息泄露之配置不当；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；
- 12、远程代码执行漏洞的探讨；
- 13、服务器安全管控的探讨。



 jsrc_team

 京东安全应急响应中心

动动手指~关注下呗~