深壁固垒--互联网暴露面收缩

中国xxx集团有限公司 张三 182xxxxxxxx

# 一、背景与目标

互联网暴露面检查主要通过人工方式，在当前收集的资产信息基础上，进一步确认和挖掘组织单位暴露在互联网的已知、未知资产，发现可能存在的安全隐患，并进行结果梳理，整理分析，提出优化建议，是安全自查的一个重要技术手段之一。

通过互联网暴露面的检查，可以更加清楚组织单位信息系统在互联网的开放程度，发现未经授权而暴露在互联网的资产，并进一步通过技术手段降低或解决发现的问题，为今后信息系统规划、建设和调整提供参考依据、并能够增加攻击者的攻击难度。

# 二、整体收缩思路

分析材料主要来自以下：

资产识别表/梳理表；组织单位敏感信息关键字；各类工具扫描及人工检查的结果；网络负责人的访谈和沟通的结果。

暴露面检查主要从以下5个方面作为参考点进行分析：

1. 互联网IP地址及域名
2. 端口服务
3. 应用
4. web应用
5. 敏感信息

# 暴露面收缩具体实施方法与处置方法

**域名、IP：**

--参考资产梳理中互联网IP地址表；

--务必结合网络拓扑，【客户名称】团队访谈确认所有出口IP信息，不得遗漏

--搜索引擎查找：site:xxx.com（概率较小）

--通过网站获取：微步、站长工具、DNSDUMPSTER（https://dnsdumpster.com/）、censys.io

--工具爆破：fierce、dnsdict6、Layer子域名挖掘机

1. 根据检查结果，确认无归属域名及其对应的服务器，应用等信息，补充至资产识别表的DMZ区资产表中。
2. 根据检查结果，确认无归属IP及其相关信息，补充至资产识别表的互联网IP地址中。
3. 使用CDN技术。

**端口服务：**

--参考资产识别表中的端口映射表

--使用TSS工具的资产识别功能

--使用nmap，masscan等工具进行交叉验证

--人工测试扫描结果的准确性

1、针对高危端口，和运维团队确认用途及对外开放的必要性。http，https，ftp，smtp，pop3，radius，rdp，telnet，ssh，各类数据库端口，ssh，各类应用端口（jboss，websphere，weblogic）。尽可能关闭非必要性对外开放端口，减少暴露面。

**应用：**

--堡结合资产收集表中的网络拓扑图、端口映射表和网络，安全产品清单进行初步收集

--与【客户名称】团队访谈进行确认

1、VPN、堡垒机、云桌面等应用管理控制台、后台不得对互联网开放。

2、VPN、堡垒机、云桌面检查用户认证是否采用双因素认证，是否启用密码复杂度，是否开启防爆破功能，是否对接入用户进行权限划分等。

**Web应用：**

--针对端口识别服务，检测指纹并梳理出web应用

--针对梳理出的web应用，结合TSS扫描工具，资产梳理表和运维团队访谈的结果，确认技术架构（脚本语言，数据库，web框架），内容管理系统（例如：wordpresss，joomla等）

--针对梳理出的web应用，和业务系统人员确认web后台管理页面，用户登录页面

1、非必要对外开放的web业务进行关闭。

2、关闭非必要对外开放的web应用端口，如weblogic的7001、5566，tomcat、jboss的8080，webshere的9080。

3、关闭所有对外开放的web管理后台页面；对外开放的web用户登录页面应检查是否具备防爆破能力，是否加入安全设备的防爆破保护模块部署Waf防止恶意爬虫，目录扫描等违规操作。

**源代码：**

--通过御剑等后台扫描工具，使用备份文件名字典进行扫描

--根据与【客户名称】提供的关键字在github等代码分享、托管平台进行搜索查寻

--通过各种云盘进行搜索查寻

1. 对于扫描发现的网站后台备份文件，并进行清除。
2. 对于在github等代码托管平台发现的源代码泄露事件，追究责任人并进行清除。

# 四、暴露面收缩成果

临战前，我方根据最新梳理的资产清单，共对虚拟化服务器资产xx台、物理服务器xx台进行存活扫描，经确认虚拟化服务器存活xx台，物理服务器存活xx台。

梳理负载均衡设备对外发布的IP、端口及其对应的业务共计xx条。与业务人员逐一核实对外发布业务，筛选出涉及高危端口的映射、非核心业务的映射共计xx条。

梳理互联网防火墙的域间策略xx条、ACL策略xx条，筛选出涉及高危端口的策略1xx条，批量放通的策略xx条。

梳理包含虚拟机、物理机的内网业务服务器xx台，筛选出非核心业务虚拟机xx台，非核心业务物理服务器xx台。

使用Nmap端口扫描工具、FOFA搜索引擎，分别对铁通xx个IP地址段、联通xx个地址段、电信xx个地址段、移动xx个地址段进行扫描，共发现xx个暴露互联网资产，经确认均为【客户名称】系统无误。

护网临战阶段，通过FOFA搜索引擎对股份公司暴露在互联网的资产再次进行搜索，共发现3个关于股份公司暴露互联网资产，经确认1个系统为公司资产，并对其进行暴露面收敛。

# 五、后续工作与补充

端口存活性探测的准确性会受扫描设备运行状态，网络环境等因素影响，建议对扫描结果进行人工验证，同时结合多种扫描工具（nmap，masscan）交叉验证，尽可能不出现漏端口或者服务的情况。

# 六、总结成效

互联网暴露面缩小后，减少了攻击者在信息收集阶段获取的信息，增加攻击者的攻击难度；同时也方便进行互联网暴露资产的漏洞自查和修复，其实互联网暴露面收缩本质上也是资产梳理的一部分，是对互联网资产的专项梳理，只有摸清家底，才能完善管理。