针对定向网络攻击主要风险分析访谈检查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **分类** | **测评项** | **风险描述** | **检查项** | **检查结果** | **整改建议** |
| 互联网入口攻击 | 应用网站安全漏洞 | 应用系统和网站存在高风险安全漏洞，可能直接被攻击者利用，从而直接或间接获取服务器权限，进而对系统及内部网络进行攻击。 | 应用系统上线前是否进行源代码审计 | 🞎是 🞎否 | 定期开展渗透测试，上线前进行代码审计，针对发现的漏洞要全面整改类似漏洞，不能只单点修复报告中的问题 |
| 应用系统是否定期开展渗透测试工作 | 🞎是 🞎否 |
| 针对发现的漏洞是否定期修改 | 🞎是 🞎否 |
| 弱口令、默认口令 | 互联网可以访问的网站系统、应用系统或管理后台等，如果其用户使用弱口令或默认口令（厂商初始化口令），可以轻易被攻击者猜测、破解，进而上传后门、获取权限，获得互联网攻击入口 | 互联网用户主机是否存在弱口令 | 🞎是 🞎否 | 修改所有用户弱口令和默认口令，要求应用系统和中间件等开启口令策略，口令须满足复杂度要求并定期更换。 |
| 是否开启口令复杂度要求 | 🞎是 🞎否 |
| 应用和中间件管理后台暴露 | 网站应用系统后台或中间件管理后台对互联网开放，攻击者可对其进行攻击，利用漏洞或破解口令，获取后台权限，进而上传后门、获取权限，获得互联网攻击入口 | 是否允许互联网访问应用管理后台 | 🞎是 🞎否 | 全面排查向互联网暴露的资产是否存在管理后台，利用防火墙等关闭管理后台互联网访问，并按照最小化原则开放后台访问权限。 |
| 是否针对管理后台开启严格的访问权限控制 | 🞎是 🞎否 |
| 是否针对管理后台访问权限进行限制 | 🞎是 🞎否 |
| 服务器互联网暴露 | 服务器应只向互联网开放业务所需的http和https等端口，如服务器向互联网暴露了过多端口，极易被攻击者攻击，攻击者可直接控制服务器，进而对内部网络进行跳板攻击。 | 对外网开放端口是否存在危险端口，如3389、445等 | 🞎是 🞎否 | 采用资产发现全面排查向互联网暴露的资产和开放的端口，同时梳理防火墙策略，对互联网开放的服务器多余端口进行关闭。 |
| 防火墙策略限制粒度是否为端口级 | 🞎是 🞎否 |
| 服务器外联风险 | 所有服务器，包括DMZ和应用、数据库服务器等，均应禁止访问互联网，如开放了向互联网访问的策略，攻击者可通过建立反向代理等方式远程控制服务器，进而对内部网络进行扩散攻击，通过获取口令远程控制服务器，利用此服务器对同一网络区域进行跳板攻击，类似这样的攻击场景，安全设备基本无法监测和防护。 | 服务器是否针对互联网开放访问权限 | 🞎是 🞎否 | 对所有服务器关闭互联网访问权限，如因业务需要开放，应按照最小化原则，只针对特定ip开放特定端口 |
| 若对外开放，是否开启严格的访问控制，限制特定IP进行访问。 | 🞎是 🞎否 |
| 内部网络横向攻击 | 弱口令、默认口令 | 内部网络资产如使用弱口令、默认口令，极易被攻击者利用跳板机攻击控制，进而扩大攻击面，特别是运维使用的管理系统，包括堡垒机、网管系统、域控等，其权限很大并包含了大量的管理数据，被攻击者控制会造成重大风险。 | 内部网络资源是否存在弱口令及默认口令？ | 🞎是 🞎否 | 全面排查修改内部网络弱口令和默认口令，包括管理系统、服务器、网络设备和安全设备等，特别是管理系统，要求开启口令策略，口令须满足复杂度要求并定期更换。 |
| 管理系统设备是否开启口令复杂度要求 | 🞎是 🞎否 |
| 设备使用同一口令 | 为方便记忆和使用，网络内大量设备使用同样的一个或几个口令，如口令被攻击者破解或获取，攻击者可以利用口令直接获取大量设备的权限，且因未发起网络攻击，安全设备很难监测告警。 | 网络内设备是否为同一口令 | 🞎是 🞎否 | 全面排查网络内设备的口令，对同一口令进行修改，要求开启口令策略，口令须满足复杂度要求并定期更换。 |
| 是否开启口令复杂度要求 | 🞎是 🞎否 |
| 操作系统、中间件安全漏洞 | 操作系统或中间件存在高风险漏洞，如weblogic反序列化、struts2漏洞、永恒之蓝漏洞等，攻击者可以从跳板机直接发起攻击，获得操作系统控制权限。在安全域划分完善、访问控制严格的网络中，中间件漏洞可能成为攻击者横向扩散的一个有效利用点，攻击者利用漏洞通过业务端口控制其它网段服务器，绕过网络访问控制。 | 针对系统及中间件等是否定期进行安全补丁更新 | 🞎是 🞎否 | 全面扫描系统和中间件漏洞并对高风险漏洞及时整改，建立定期漏洞扫描和整改追踪机制，确保高风险漏洞切实整改。 |
| 针对系统及相关软件是否定期进行漏洞扫描 | 🞎是 🞎否 |
| 针对发现的漏洞是否进行整改追踪 | 🞎是 🞎否 |
| 内部系统安全漏洞 | 部分对内部开放的应用系统，攻击者取得跳板机后会对这些系统进行攻击测试，如系统存在安全漏洞，可被攻击者利用获取系统权限并控制服务器。对于内部系统，应和互联网系统同等对待，同样可能直接面临攻击者的攻击测试。 | 针对内部系统是否定期开展渗透测试 | 🞎是 🞎否 | 定期对内部系统开展渗透测试，上线前进行代码审计，针对发现的漏洞要全面整改类似漏洞，不能只单点修复报告中的问题。 |
| 内部系统上线前是否经过代码审计 | 🞎是 🞎否 |
| 针对发现的问题进行是否全面整改 | 🞎是 🞎否 |
| 集权类系统风险和要求 | 邮件服务器 | 邮件服务器若被外部攻击攻陷，则整个邮件服务器内保存的邮件信息则可被攻击者获取，可能会从其中获得隐藏在邮件中的敏感信息，如服务器口令，相关责任人信息，攻击者可通过此类信息进行下一步攻击。 | 口令，敏感文件等敏感信息是否禁止通过邮件方式传递 | 🞎是 🞎否 | 严禁在邮件中发送含敏感系统信息，包括但不限于网络拓扑架构、业务系统相关信息、服务器系统密码、服务器系统SSH密钥等，邮件系统与DMZ区ACL严格隔离。 |
| 域控制器服务器(Domain Controller)/DNS服务器/备份服务器 | 域控制服务器等服务器权限较大服务器一旦被攻击者获得权限，可能会造成及其严重影响，如相关访问控制策略被删除，DNS服务被修改，备份信息被删除等。 | 针对系统是否定期安装安全补丁 | 🞎是 🞎否 | 定时更新系统补丁、强制定时更改域控管理员及krbtgt账号密码，且采用大小写数字特殊字符混合，密码位数不低于16位（三个月强制修改一次，不能采用历史密码）。 |
| 是否定期修改管理员口令 | 🞎是 🞎否 |
| 管理员口令是否开启复杂度要求 | 🞎是 🞎否 |
| ITSM运维管理系统/Zabbix/Nagios/堡垒机等集成监控维护系统 | 相关集成监控维护系统及服务器权限较大，若被攻击者攻击并获得管理权限后，会造成极大影响，修改相关系统权限，获得服务器口令，甚至是控制全部监控维护系统下服务器权限。 | 是否针对重要集成监控维护服务器配置严格ACL进行严格控制 | 🞎是 🞎否 | 严格ACL访问控制，细化ACL规则，不同服务器采用不同的复杂且随机的密码，密码位数不低于16位的密码。严格限制以上系统后台/控制台对外开放，建议仅开放特定用户、特定IP访问以上系统后台/控制台。 |
| 重要集权系统是否为相同口令 | 🞎是 🞎否 |
| 是否开启管理员密码口令复杂度要求 | 🞎是 🞎否 |
| 是否针对访问IP进行限制 | 🞎是 🞎否 |
| 研发服务器/SVN/Git  | 相关研发服务器、SVN、Git等相关管理服务器权限较大或存放重要信息，若被攻击者攻击，会造成数据泄露，权限被恶意变更等严重事件。 | 是否针对重要服务器配置严格ACL进行严格控制 | 🞎是 🞎否 | 严格ACL访问控制，研发服务器/SVN/Git等服务器仅开放特定IP访问，如研发个人终端访问，同时建议访问服务器时采用双因素认证，如USBKey等。 |
| 针对重要服务器是否开启访问控制权限 | 🞎是 🞎否 |
| 是否针对访问服务器人员的身份进行双因子鉴定 | 🞎是 🞎否 |
| 研发个人终端/运维个人终端 | 相关研发及运维人员终端所处的网段或IP权限较大，拥有访问相关重要信息系统服务器，若终端被黑为“肉鸡”，则攻击者可远程控制终端进行攻击行为甚至是破坏行为。 | 终端是否安装杀毒及安全防护软件并定期更新病毒库及防护规则 | 🞎是 🞎否 | 建议细化ACL规则，定时更新系统补丁、查杀病毒、定时修改系统密码、提高研发运维人员安全意识等。 |
| 终端是否定期更改管理员密码 | 🞎是 🞎否 |