什么是渗透测试?

> 渗透测试(**Penetration Test**):是完全模拟黑客可能使用的攻击技术和漏洞发现技术,对目标系统的安全做深入的探测,发现系统最薄弱的环节.渗透测试能够直观的让管理人员知道自己网络所面临的问题
>
> **渗透测试是一种专业的安全服务**

1. **国际渗透测试标准:OWASP**
2. **国际渗透测试标准:OSSTMM**
3. **国际渗透测试流程:PTES**
4. **Web安全测试规范**

渗透测试中必须要需要的声明

保密协议

附件一：保密协议书

保 密 协 议 书

鉴于乙方接受甲方委托，将在合同规定的期限内为甲方提供测评服务，而在提供服务过程中，乙方将不可避免地接触到甲方的技术资料及数据信息，为落实保密措施，做好保密工作，切实维护甲方的利益，双方就有关保密事宜达成如下意见：

一、甲方职责

1、甲方应对乙方以及乙方明确为甲方提供测评服务的人员进行保密责任、保密义务提醒教育，并对乙方测评服务人员进行测评服务具体实施进行全程跟踪、监督和管理。

2、对于乙方提出的与测评服务密切相关且必须提供保密资料等相关事宜进行保密审查认证，并对提供给乙方的相关保密资料提出比较明确的保密要求，做好交接登记工作。

3、发现乙方在为甲方实施测评服务过程中存在安全隐患和泄密漏洞的，应当及时提出，并督促落实改进措施，确保安全。

二、乙方职责

1、乙方在接受甲方委托之日起，应当事先做好相关准备工作：一是明确具体负责测评服务的人员，且做到相对固定；二是对相关测评服务人员进行保密教育，明确保密责任、义务；三是做到持证上岗(确认身份)。因测评服务需要增加的相关人员，按同等要求落实相关措施。

2、乙方测评服务人员在为甲方提供测评服务过程中，应尽量避免接触甲方的工作秘密事项，做到不该看的不看，不该问的不问；因提供测评服务需要必须

接触工作秘密事宜时，应主动接受甲方的现场指导和监督，并确保有关设备和信息的安全。

3、乙方在为甲方提供测评服务时，甲方根据乙方提出的要求，必须提供保密资料时，双方应当办理交接手续，做好登记、使用台帐；乙方在将相关保密资料带回使用时，应确保携带、使用、存放全过程的安全；保密资料不得另行复制，确因测评服务需要经甲方书面同意复制的，按原件要求严格管理。

4、乙方在完成甲方某项测评服务任务后，与此任务相关、且短期内不再使用的先前甲方提供的保密资料，应先期退回甲方，并办理保密资料退回手续，做好交接登记。甲方认为可以作废不需退回的保密资料，乙方应当及时进行保密销毁，并做好核销登记。

5、乙方对于甲方提供的保密资料以及相关测评服务人员在为甲方提供测评服务时掌握的其他数据信息，均不得向第三方或其他无关人员透露，应按照测评服务需要严格控制使用、知悉范围。

6、乙方在使用电子设备(包括笔记本电脑、移动存储介质等)为甲方提供测评服务时，应严格按照国家有关保密规定要求，落实技防、人防、物防综合防范措施，确保安全。

三、违约与赔偿

1、任何一方违反本协议的规定，应在第一时间采取一切必要措施防止保密信息的扩散，尽最大可能消除影响，并应承担违约责任，向守约方支付违约金，违约金的具体数额为双方合作项目金额的 5 %（或由双方协商确定）。

2、上述违约金数额并不影响受损害方向违约方要求损害赔偿。该赔偿以受损害方实际遭受的损失为限。

四、其他事宜

1、由于违反约定，造成泄密事件发生或者产生严重泄密隐患的，由违约一方承担全部责任。

2、乙方对接触到甲方的数据信息及保密资料等严格落实保密措施，确保乙方及乙方工作人员做好保密工作，如因乙方及乙方工作人员原因导致泄密或存在严重泄密隐患的，应承担相应的保密责任，赔偿相关损失。

3、未尽事宜，双方另行择机商定。

甲 方：

法定代

签 字：

乙方：（

法定代

签字：

渗透测试授权书

开展渗透测试工作前,必须与测试单位签订《渗透测试授权书》

授权书

我单位在知悉、理解并接受渗透测试和漏洞扫描过程中可能产生的影响和风险情况下，授权某某信息技术有限公司（下称“某某”）对我单位提供渗透测试、漏洞扫描及修复建议。

授权期间为 2020 年 07 月 28 日至 2020 年 07 月 28 日。

在授权期间，双方可以电子授权函形式补充确认授权，电子授权函作为本授权函补充，具同等法律效力。

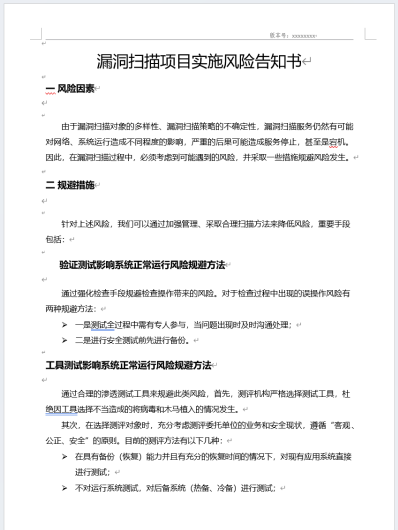
双方就本授权函及授权行为下产生的相关数据信息应承担保密义务，不应以任何方式将相关信息泄露给第三方。

----------（以下无正文）----------

单位名称：（盖章）_____

日期：2020.07.28

风险告知书



漏洞扫描项目实施风险告知书

一 风险因素

由于漏洞扫描对象的多样性、漏洞扫描策略的不确定性，漏洞扫描服务仍然有可能对网络、系统运行造成不同程度的影响，严重的后果可能造成服务停止，甚至是宕机。因此，在漏洞扫描过程中，必须考虑到可能遇到的风险，并采取一些措施规避风险发生。

二 规避措施

针对上述风险，我们可以通过加强管理、采取合理扫描方法来降低风险，重要手段包括：

验证测试影响系统正常运行风险规避方法

通过强化检查手段规避检查操作带来的风险。对于检查过程中出现的误操作风险有两种规避方法：

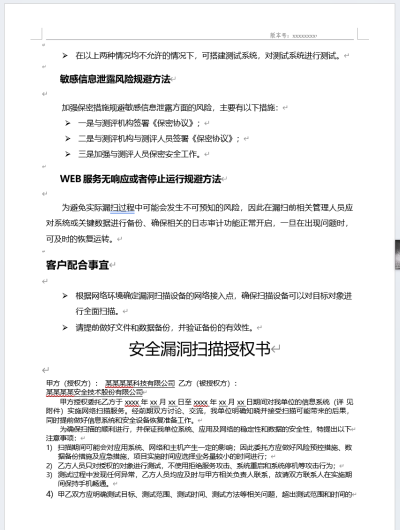
- 一是测试全过程中需有专人参与，当问题出现时及时沟通处理；
- 二是进行安全测试前先进行备份。

工具测试影响系统正常运行风险规避方法

通过合理的渗透测试工具来规避此类风险，首先，测评机构严格选择测试工具，杜绝因工具选择不当造成的病毒和木马植入的情况发生。

其次，在选择测评对象时，充分考虑测评委托单位的业务和安全现状，遵循“客观、公正、安全”的原则。目前的测评方法有以下几种：

- 在具有备份（恢复）能力并且有充分的恢复时间的情况下，对现有应用系统直接进行测试；
- 不对运行系统测试。对后备系统（热备、冷备）进行测试；



- 在以上两种情况均不允许的情况下，可搭建测试系统，对测试系统进行测试。

敏感信息泄露风险规避方法

加强保密措施规避敏感信息泄露方面的风险，主要有以下措施：

- 一是与测评机构签署《保密协议》；
- 二是与测评机构与测评人员签署《保密协议》；
- 三是加强与测评人员保密安全工作。

WEB 服务无响应或者停止运行规避方法

为避免实际漏扫过程中可能会发生不可预知的风险，因此在漏扫前相关管理人员应对系统或关键数据进行备份，确保相关的日志审计功能正常开启，一旦在出现问题时，可及时的恢复运转。

客户配合事宜

- 根据网络环境确定漏洞扫描设备的网络接入点，确保扫描设备可以对目标对象进行全面扫描。
- 请提前做好文件和数据备份，并验证备份的有效性。

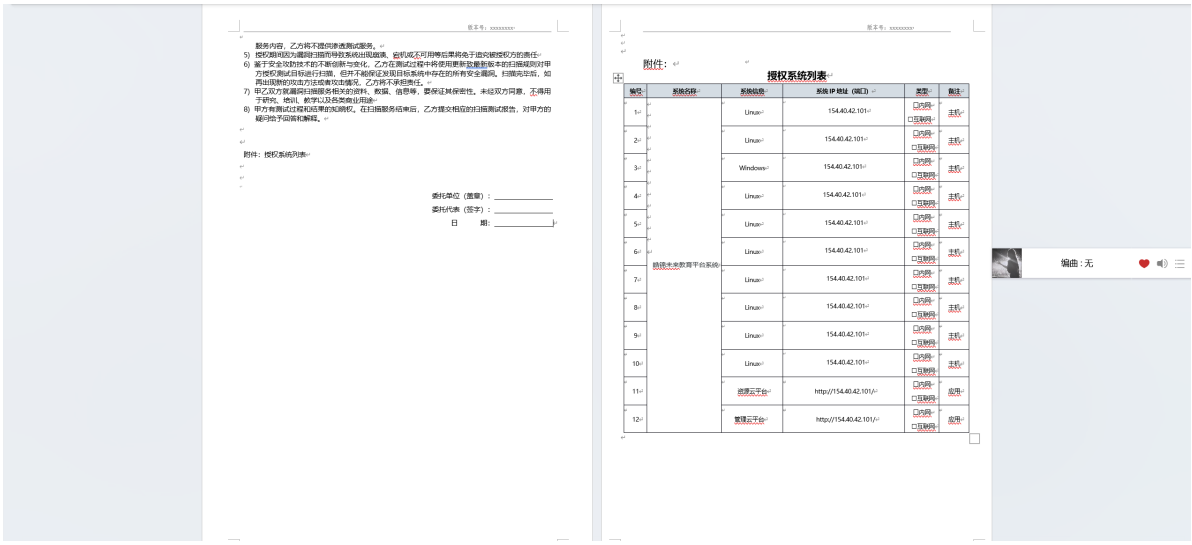
安全漏洞扫描授权书

甲方（授权方）：某某某某科技有限公司 乙方（被授权方）：某某某某安全技术股份有限公司

甲方授权委托乙方于 xxxx 年 xx 月 xx 日至 xxxx 年 xx 月 xx 日期间对我单位的信息系统（详见附件）实施网络扫描服务，经双期双方讨论、交流，我单位明确知晓并接受扫描可能带来的后果，同时提前做好信息系统和安全设备恢复准备工作。

为确保扫描的顺利进行，并保证我单位系统、应用及网络的稳定性和数据的安全性，特提出以下注意事项：

1) 扫描期间可能会对应用系统、网络和主机产生一定的影响；因此委托方应做好风险预控措施，数据备份措施及应急措施，原则上实施时间应选择业务量较少时的时间进行；
2) 乙方人员只对授权的对象进行测试，不使用拒绝服务攻击，系统漏洞扫描机禁攻击行为；
3) 测试过程中发现任何异常，乙方人员均应及时与甲方相关负责人联系，故请双方联系人在实施期间保持手机畅通。
4) 甲乙双方应明确测试目标、测试范围、测试时间、测试方法等相关问题，细出测试范围和时间的

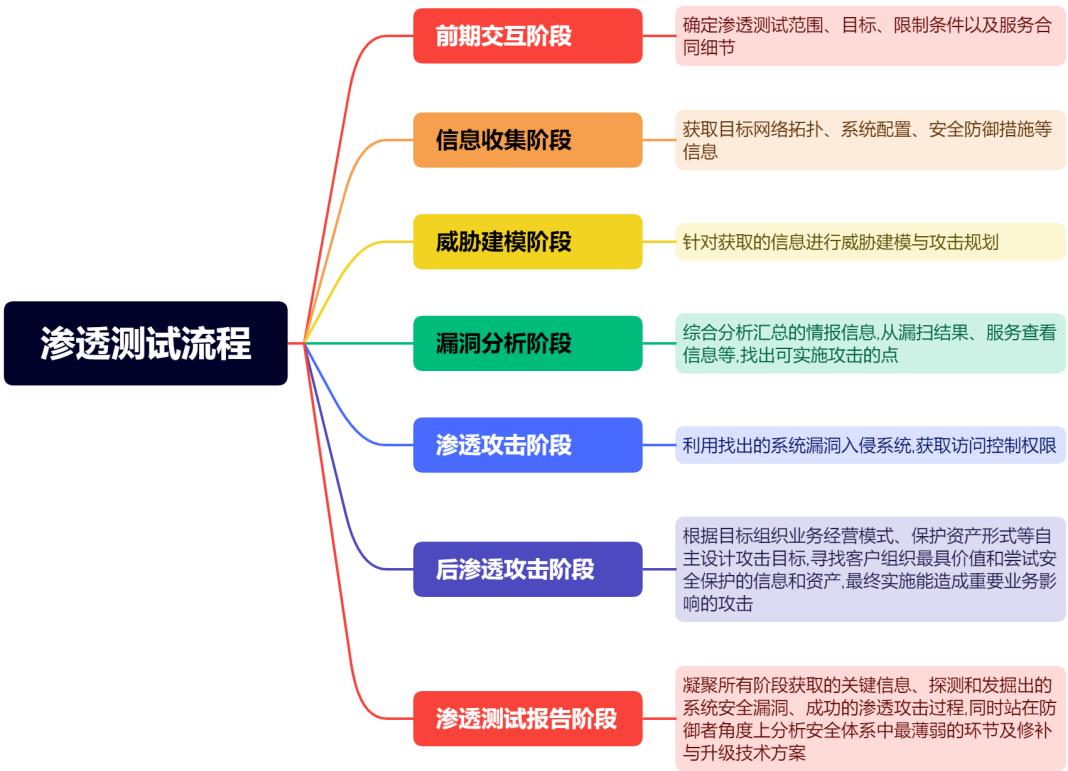


渗透测试与入侵的区别

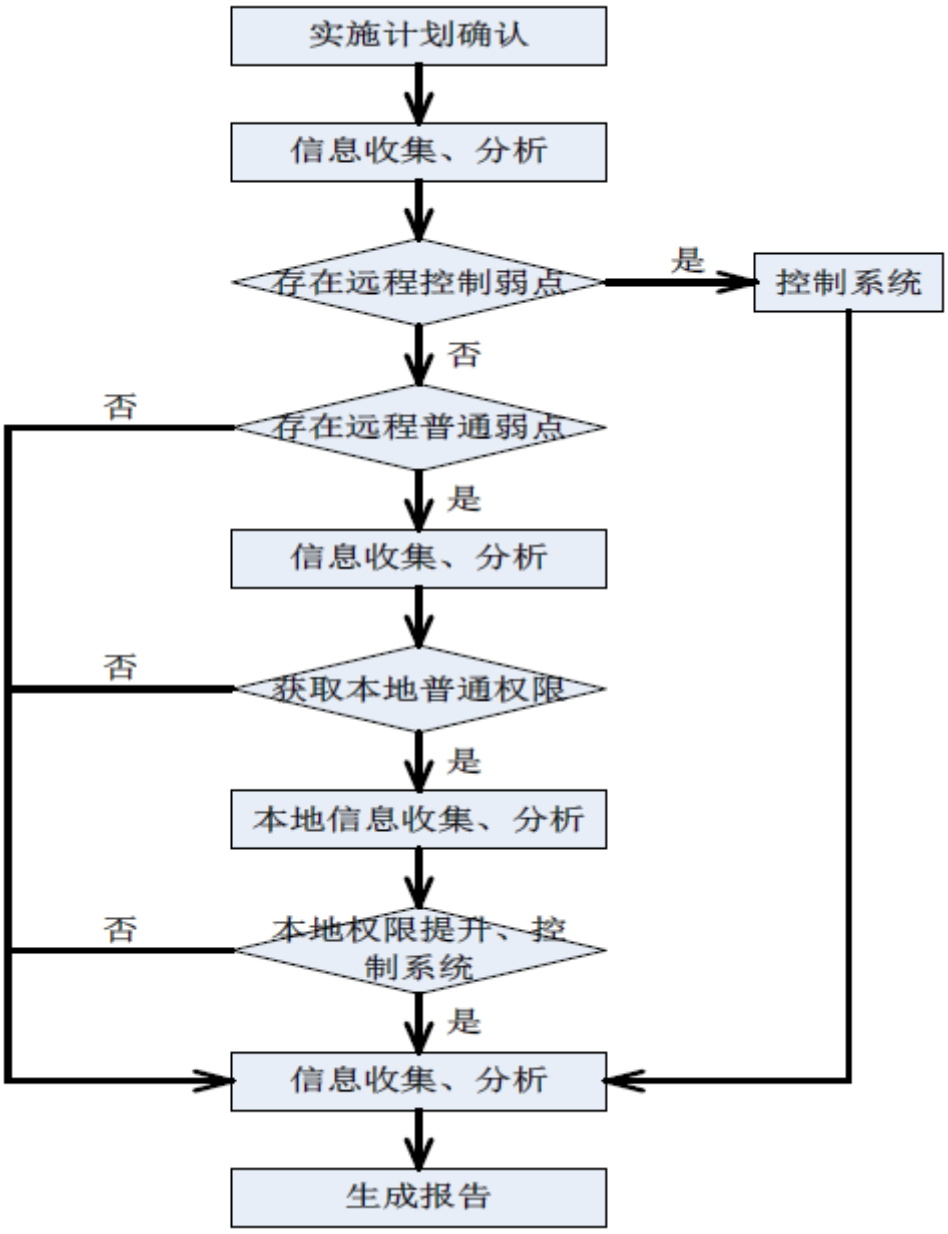
渗透测试:以安全为基本原则，通过攻击者以及防御者的角度去分析目标所存在的安全隐患以及脆弱性，以保护系统安全为最终目标。

入侵:通过各种方法，甚至破坏性的操作，来获取系统权限以及各种敏感信息。

一般渗透测试流程(PTES)



、



测试方法:

1. 黑盒测试
    - 它是指在测试过程中，测试人员没有或只有很少的关于被测试系统的内部结构、工作原理和代码实现等信息。测试人员只能通过系统对外部接口的输入和输出来判断系统是否存在安全漏洞。 黑盒测试通常是在测试人员不了解系统内部结构和源代码的情况下进行的，这种测试方法更加贴近于实际的攻击情况，因为攻击者通常也无法获得系统的内部信息。黑盒测试可以模拟攻击者的行为来测试系统的安全性，包括但不限于输入验证、身份认证、访问控制、数据加密、会话管理、错误处理等方面。 黑盒测试可以帮助组织评估其系统的安全性，以及找出其中的弱点和漏洞，以便采取措施加以弥补。同时，黑盒测试也可以帮助组织提高其系统的安全性，以保护系统中的敏感信息不被攻击者获取。
2. 白盒测试
    - 它是指在测试过程中，测试人员拥有被测试系统的内部结构、工作原理和代码实现等信息。测试人员可以利用这些信息来测试系统是否存在安全漏洞。 白盒测试通常是在测试人员已经了解系统内部结构和源代码的情况下进行的，这种测试方法可以更加全面地检查系统的安全性。白盒测试可以检查系统的代码实现是否符合安全标准和最佳实践，包括但不限于输入验证、身份认证、访问控制、数据加密、会话管理、错误处理等方面。 白盒测试可以帮助组织评估其系统的安全性，以及找出其中的弱点和漏洞，以便采取措施加以弥补。同时，白盒测试也可以

帮助组织提高其系统的安全性，以保护系统中的敏感信息不被攻击者获取。白盒测试的优势在于可以发现一些黑盒测试无法发现的细节性问题，但它需要测试人员具备丰富的技术和经验。

3. 灰盒测试
    - 是一种介于黑盒测试和白盒测试之间的测试方法，它是指在测试过程中，测试人员有一定的关于被测试系统的内部结构、工作原理和代码实现等信息，但这些信息通常不够详细或完整。测试人员可以利用这些信息来测试系统是否存在安全漏洞，同时也需要模拟攻击者的行为来测试系统的安全性。 灰盒测试通常是在测试人员了解系统的某些部分内部结构和源代码的情况下进行的，但测试人员通常无法完全了解系统的所有部分。灰盒测试可以结合黑盒测试和白盒测试的优势，既可以测试系统的输入输出接口，又可以检查系统的代码实现是否符合安全标准和最佳实践。同时，灰盒测试也可以模拟攻击者的行为来测试系统的安全性。 灰盒测试可以帮助组织评估其系统的安全性，以及找出其中的弱点和漏洞，以便采取措施加以弥补。同时，灰盒测试也可以帮助组织提高其系统的安全性，以保护系统中的敏感信息不被攻击者获取。灰盒测试需要测试人员具备丰富的技术和经验，以便在了解系统的一定部分内部结构和源代码的情况下，能够全面地测试系统的安全性。
4. 人工测试
    - 它是指由专业的安全测试人员通过手动操作、模拟攻击等方式来测试系统的安全性。测试人员会利用各种技术手段和攻击方法来检测系统的安全性，并尝试发现系统中可能存在的安全漏洞、弱点或潜在风险。 信息安全人工测试通常包括黑盒测试、白盒测试和灰盒测试等多种测试方法，测试人员可以根据系统的特点和测试目标选择合适的测试方法。测试人员需要具备丰富的安全知识和技能，能够模拟攻击者的行为来测试系统的安全性，并能够准确地分析系统中可能存在的安全风险和漏洞。 信息安全人工测试可以帮助组织评估其系统的安全性，以及找出其中的弱点和漏洞，以便采取措施加以弥补。同时，信息安全人工测试也可以帮助组织提高其系统的安全性，以保护系统中的敏感信息不被攻击者获取。信息安全人工测试需要测试人员具备丰富的技术和经验，以便能够全面地测试系统的安全性，并提供有效的测试报告和建议。
5. 工具扫描
    - 它是指利用专业的安全扫描工具，对系统的漏洞、弱点等进行自动化扫描，以检测系统是否存在安全漏洞。信息安全工具扫描通常包括漏洞扫描、端口扫描、Web应用程序扫描等多种扫描方法，测试人员可以根据系统的特点和测试目标选择合适的扫描方法。 信息安全工具扫描可以帮助组织快速地扫描系统的安全性，发现系统中可能存在的安全漏洞、弱点或潜在风险。扫描工具可以自动化地进行扫描，减轻测试人员的工作量，并提高测试的效率。同时，扫描工具还可以提供详细的扫描报告和建议，以帮助组织了解系统的安全状况，并采取相应的措施加以弥补。 虽然信息安全工具扫描可以快速地发现系统中的安全漏洞，但它也存在一定的局限性。扫描工具可能会误报或漏报某些漏洞，因此测试人员需要对扫描结果进行人工验证。同时，扫描工具只能检测已知的漏洞，对于新型的或未知的漏洞可能无法进行检测。因此，信息安全工具扫描应该与其他测试方法结合使用，以提高测试的准确性和全面性。
6. 漏洞验证
    - 它是指在发现系统中存在安全漏洞后，通过模拟攻击等方式来验证漏洞的存在性和危害性。漏洞验证的过程通常包括漏洞重现、漏洞利用、攻击模拟和影响评估等步骤。 在进行信息安全漏洞验证之前，测试人员需要对漏洞进行详细的分析和确认，确定其存在性和危害性，以避免对系统造成不必要的损失。漏洞验证需要测试人员具备丰富的安全知识和技能，能够模拟攻击者的行为来测试系统的安全性，并能够准确地分析漏洞的危害性和可能的攻击手段。 信息安全漏洞验证可以帮助组织评估其系统的安全性，以及找出其中的弱点和漏洞，以便采取措施加以弥补。同时，漏洞验证也可以帮助组织提高其系统的安全性，以保护系统中的敏感信息不被攻击者获取。漏洞验证的结果可以帮助组织更好地了解漏洞的危害性，并采取相应的措施加以修复和防范。 需要注意的是，在进行信息安全漏洞验证的过程中，测试人员需要遵守相关的法律法规和道德规范，不得进行未授权的攻击行为，以免对系统造成不必要的损失。
7. 漏洞演示

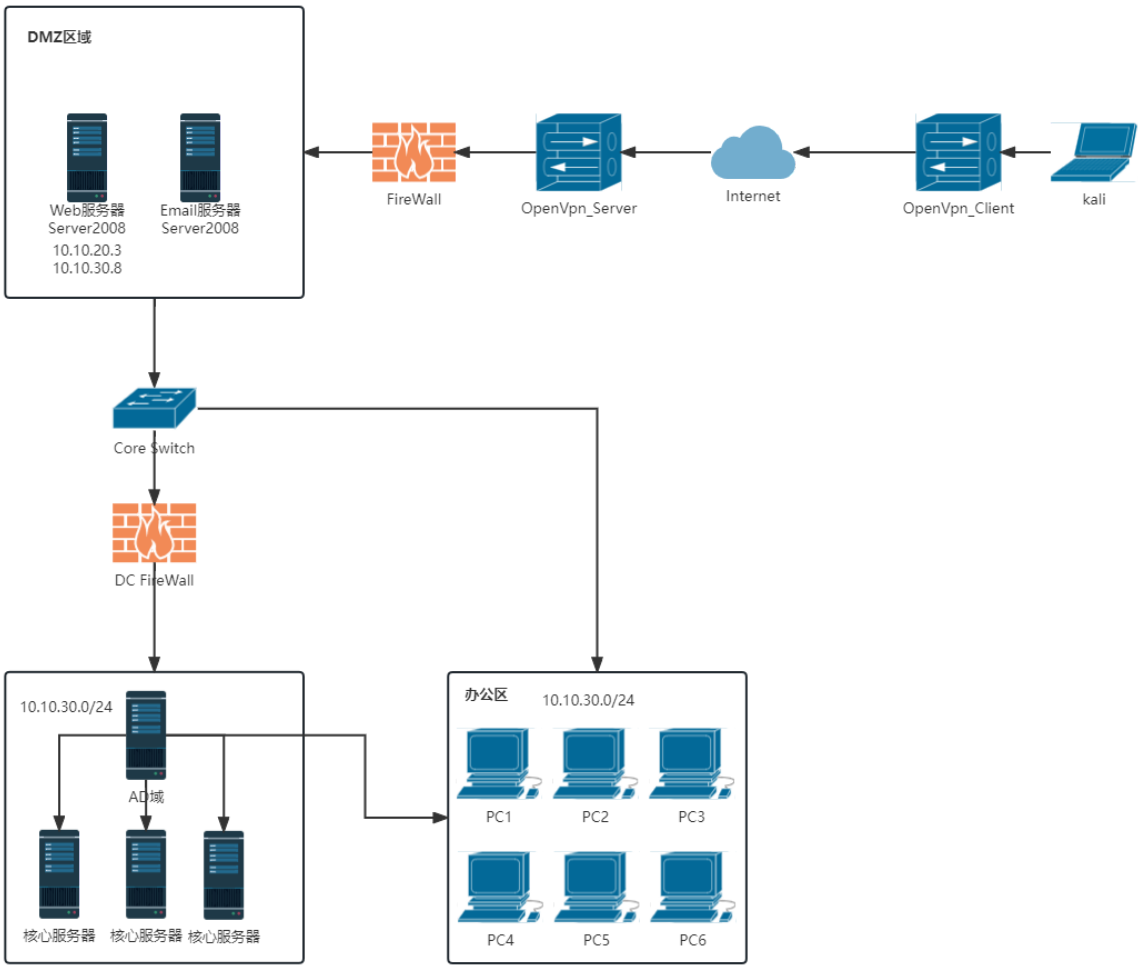
- 它是指在验证系统中存在安全漏洞后，通过演示来展示漏洞的存在性、危害性和攻击手段。漏洞演示通常包括利用漏洞进行攻击、获取敏感信息、篡改数据等多种攻击场景，以呈现漏洞的真实危害性，并帮助组织更好地了解漏洞的危害性和防范措施。 信息安全漏洞演示需要演示人员具备丰富的安全知识和技能，能够准确地模拟攻击者的行为，演示攻击的全过程，并能够解释漏洞的危害性和防范措施。漏洞演示需要演示人员提前进行充分的准备和测试，以确保演示的顺利进行，并避免因漏洞演示而对系统造成不必要的损失。 信息安全漏洞演示可以帮助组织更好地了解漏洞的危害性和攻击手段，以及采取相应的措施加以修复和防范。漏洞演示可以提高组织对安全风险的认识和意识，增强组织的安全意识和防范能力。同时，漏洞演示还可以帮助组织评估其信息安全的水平和风险状况，制定和完善相应的安全策略和规范，以保障组织的信息安全。

8. 横向渗透

- 横向渗透（Lateral Movement）是指攻击者在已经入侵了一台或多台受害者主机之后，通过利用系统漏洞、弱口令等方式，向网络中其他主机进行攻击，并在网络中横向移动，以获取更多的系统权限和敏感信息。攻击者通常会使用恶意软件、后门程序等手段来进行横向渗透，以避免被系统安全软件和检测机制发现和拦截。 横向渗透对于攻击者而言非常重要，因为攻击者可以通过横向渗透在网络中获得更多的权限和敏感信息。攻击者通过横向渗透可以访问其他主机上的文件、数据库、邮件等敏感信息，甚至可以获取系统管理员的权限，从而进一步深入系统，控制整个网络。 为了防范横向渗透攻击，组织可以采取一些安全措施，如加强系统安全配置、及时更新补丁、使用强口令、限制用户权限、使用安全软件等。此外，组织还可以通过安全培训和意识提高等方式提高员工的安全意识，减少安全漏洞的发生。

9. 纵向渗透

- 纵向渗透（Vertical Movement）是指攻击者在已经入侵了一台或多台受害者主机之后，通过利用系统漏洞或社交工程等手段，向网络中更高级别的主机或系统进行攻击，以获取更高级别的系统权限和敏感信息(**一句话概括:提权或者拿主控机器**)。攻击者通常会利用系统中的弱点和漏洞，来获取更高级别的权限和敏感信息，从而控制整个网络。 纵向渗透攻击通常是通过提升攻击者的权限来实现。攻击者可能会从普通用户的权限提升到管理员的权限，然后再提升到系统管理员的权限，最终控制整个网络。攻击者还可以通过利用社交工程等手段，获取高级别用户的账号和密码，从而进一步提升其权限。纵向渗透攻击的危害性非常大，因为攻击者可以通过提升权限来控制更多的系统资源和敏感信息，从而对受害组织造成更大的损失。 为了防范纵向渗透攻击，组织可以采取一些安全措施，如限制用户权限、加强系统安全配置、使用强口令、定期修改密码等。此外，组织还可以通过安全培训和意识提高等方式提高员工的安全意识，减少安全漏洞的发生。同时，组织还应该定期进行安全漏洞扫描和漏洞修复，以及加强日志的监控和分析，及时发现和防范纵向渗透攻击。



渗透测试价值

1. 帮助用户对目前自己的网络、系统、应用的缺陷有相对直观的认识和了解
2. 发现已知和未知的漏洞和风险,为漏洞修复和风险处置提供技术支撑
3. 给信息系统全面的体检,查找存在的风险及隐患,防患于未然