内网基础

什么是内网

是指在某一区域内由多台计算机互联成的计算机组。

内网即局域网LAN网。局域网的覆盖范围一般是方圆几千米之内，其具备的安装便捷、成本节约、扩展方便等特点使其在各类办公室内运用广泛。局域网可以实现文件管理、应用软件共享、打印机共享等功能，在使用过程当中，通过维护局域网网络安全，能够有效地保护资料安全，保证局域网网络能够正常稳定的运行。同时内网可以简单理解为私网，针对企业而言的叫内网，企业外部的叫外网。

DMZ区域是什么

是指在网络安全中用于隔离内部网络和外部网络的一块区域。

在进行渗透测试时(含内外网)，DMZ区域通常是一个攻击者可能的入口目标。攻击者可能尝试从DMZ区域入手，通过攻击DMZ中的服务器，进而进一步侵入内部网络。

安全术语

打点：信息收集以及漏洞确认阶段，一般指的是对测试/渗透目标进行信息收集，漏洞的确认。

肉鸡：所谓“肉鸡”是一种很形象的比喻，比喻那些可以被攻击者控制的电脑、手机、服务器或者其他摄像头、路由器等智能设备，用于发动网络攻击。

抓鸡： 被攻击者控制电脑的过程叫抓鸡

跳板： 一个具有辅助作用的机器，利用这个主机作为一个间接工具，来入侵其他主机，一般和肉鸡连用。

隧道： 在网络安全领域，隧道是一种通过将一种网络协议封装在另一种网络协议中进行传输的技术。它类似于在一条已有的 “管道”（基础网络连接）内再构建一条 “虚拟管道” 来传输数据。

框架：安全框架网络安全专业机构制定的一套标准、准则和程序，旨在帮助组织了解和管理面临的网络安全风险。

攻击框架是对网络攻击中所涉及的技术、战术、流程等进行系统总结和分类的模型，用于帮助安全研究人员和防御者了解攻击者的思路和方法。

C2木马： C2（Command and Control，命令与控制）木马是一种恶意软件，它允许攻击者远程控制受感染的计算机系统。木马一旦植入目标系统，就会与攻击者控制的 C2 服务器建立连接。

提权： 指得到你本没得到的权限，比如说电脑中非系统管理员就无法访问一些C盘的东西，而系统管理员就可以，通过一定的手段让普通用户提升成为管理员，让其拥有管理员的权限，这就叫提权。

后门： 这是一种形象的比喻，入侵者在利用某些方法成功的控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置，用于访问、查看或者控制这台主机。这些改动表面上是很难被察觉的，就好像是入侵者偷偷的配了一把主人房间的钥匙，或者在不起眼处修了一条暗道，可以方便自身随意进出。

shell与Webshell： Webshell和Shell都是用于远程访问目标系统的工具，但是它们的实现方式和使用方式有所不同。

Shell是一种命令行解释器，它可以让用户在终端上输入命令并执行。Shell通常是在本地计算机上安装的，并且只能在本地计算机上运行。Shell可以访问本地计算机上的文件系统和其他资源，但是它不能直接访问远程计算机的文件系统和资源。

Webshell是一种基于Web技术的后门，它可以让攻击者通过Web界面来访问远程系统。Webshell通常是通过在目标系统上安装一个Web应用程序来实现的，该应用程序可以让攻击者通过浏览器访问远程系统并执行命令。Webshell通常需要在目标系统上启用特定的服务或端口来运行，并且需要使用特定的URL或IP地址来访问它。

黑盒与白盒测试：黑盒测试又称功能测试，是将软件看作一个不透明的黑盒子，测试人员完全不考虑程序内部的逻辑结构和内部特性，只依据软件的需求规格说明书，检查程序的功能是否符合它的功能说明。

白盒测试又称结构测试，它把测试对象看作一个打开的透明盒子，测试人员需要了解程序的内部逻辑结构和处理过程，对程序的所有逻辑路径进行测试，检查程序内部操作是否按规定执行。

免杀：就是通过加壳、加密、修改特征码、加花指令等等技术来修改程序，使其逃过杀毒软件的查杀。

APT攻击：Advanced Persistent Threat，即高级可持续威胁攻击，指某组织在网络上对特定对象展开的持续有效的攻击活动。**
**这种攻击活动具有极强的隐蔽性和针对性，通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。

渗透流程

明确目标

信息搜集

漏洞探测

漏洞利用

获取立足点

权限提升

后门植入

痕迹清除

VMware虚拟机

VM0：桥接模式 桥接模式就是将主机网卡与虚拟机虚拟的网卡利用虚拟网桥进行通信。在桥接的作用下，类似于把物理主机虚拟为一个交换机，所有桥接设置的虚拟机连接到这个交换机的一个接口上，物理主机也同样插在这个交换机当中，所以所有桥接下的网卡与网卡都是交换模式的，相互可以访问而不干扰。在桥接模式下，虚拟机ip地址需要与主机在同一个网段，如果需要联网，则网关与DNS需要与主机网卡一致

VM1：主机模式 Host-Only模式其实就是NAT模式去除了虚拟NAT设备，然后使用VMware Network Adapter VMnet1虚拟网卡连接VMnet1虚拟交换机来与虚拟机通信的，Host-Only模式将虚拟机与外网隔开，使得虚拟机成为一个独立的系统，只与主机相互通讯

VM8：NAT模式 在NAT模式中，主机网卡直接与虚拟NAT设备相连，然后虚拟NAT设备与虚拟DHCP服务器一起连接在虚拟交换机VMnet8上，这样就实现了虚拟机联网。且NAT模式可以隐藏内网的虚拟机，其网卡的存在目的是为了让主机与虚拟机通信

Kali Linux

https://www.kali.org/get-kali/#kali-platforms

镜像按照教程：https://blog.csdn.net/fingue/article/details/127559353

机场平台

樱花猫：https://sakuracat-001.com/#/register?code=gXxi7oJA

FASTLINK：https://flafflnk.flaff9.cc/auth/register?code=RX0R

一元机场(备份使用)：https://xn--4gq62f52gdss.ink/#/register?code=hZGdynJ6

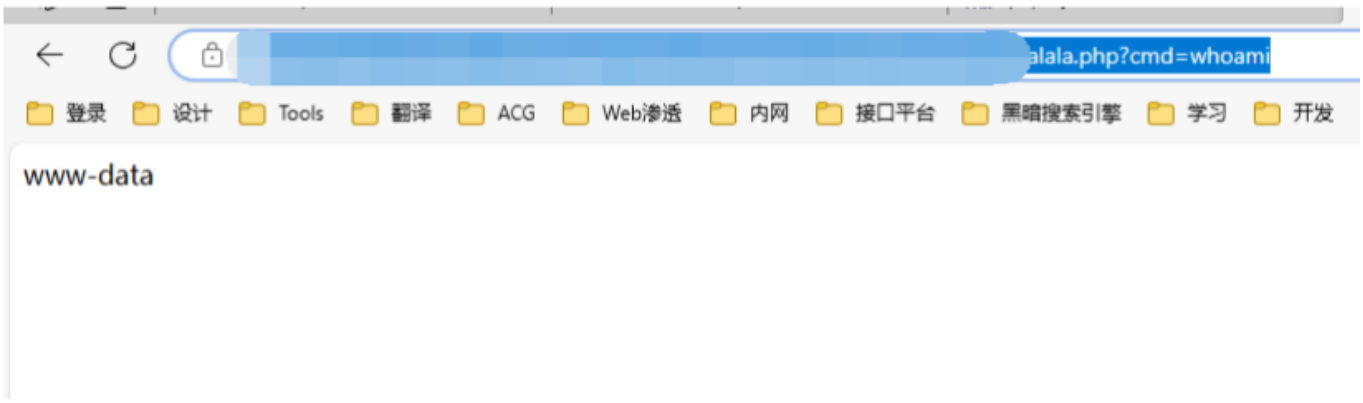
webshell权限

拿到shell以后执行whoami 命令得到用户名称

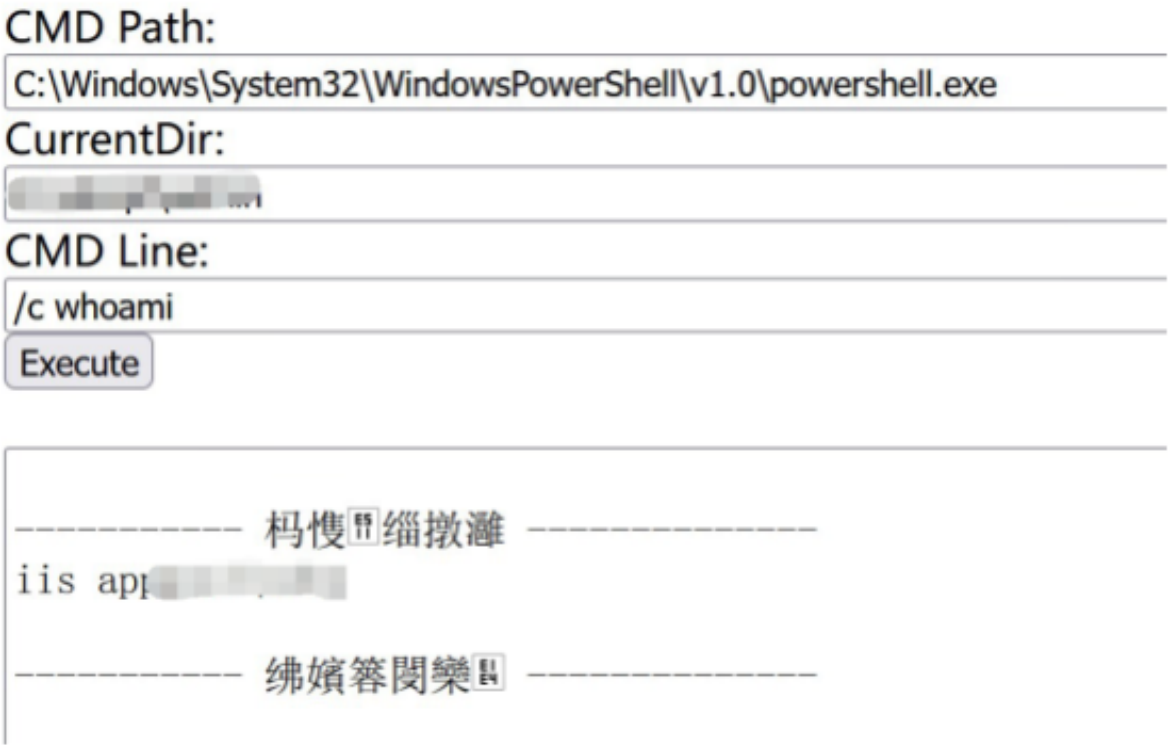
按语言来分

java： root/system （最高权限）

php： www-data （中间件的权限，很低）



aspx/asp： IIS （中间件权限，权限很低）



因为java web他运行他是独立运行，他是直接继承用户的权限，root执行那就有root

php、aspx 他们都是基于web服务器（apache、nginx、iis）去运行，权限就是继承于web服务器，apache、nginx的权限就是www-data ，IIS 就是 IIS-

靶场平台

https://www.vulnhub.com/

https://account.hackthebox.com/login

https://tryhackme.com/login

https://hackmyvm.eu/login/

红日

vulntarget：https://github.com/crow821/vulntarget

封神台

春秋云镜

云服务器

阿里云： https://www.aliyun.com/benefit

腾讯云： https://cloud.tencent.com

华为云(云耀云)： https://activity.huaweicloud.com

百度智能云： https://cloud.baidu.com

京东云： https://www.jdcloud.com

野鸡房：

3c云： https://www.3cccy.com/

云梦云： https://idc.xmcyh.cn/