名词解释

~/.ssh/*

/.ssh/* 这个命令或路径在Linux或Unix-like系统的上下文中表示的是用户主目录下的.ssh目录中的所有文件和目录。这里，代表当前用户的主目录（Home Directory），而.ssh是一个通常用于存储SSH（Secure Shell）相关配置和密钥文件的隐藏目录（因为目录名以.开头）。

.ssh目录中的常见文件和用途：

id_rsa 和 id_rsa.pub：
id_rsa：这是用户的私钥文件，用于SSH认证，应该保持私密。
id_rsa.pub：这是与id_rsa对应的公钥文件，可以安全地分享给任何需要验证你身份的服务器或服务。

authorized_keys：
这个文件包含了允许无密码登录到当前用户账户的公钥列表。通常，当你希望从某个特定的计算机（或用户）无密码登录到当前账户时，你会将那个计算机的SSH公钥添加到这个文件中。

known_hosts：这个文件包含了SSH客户端已知的主机密钥信息。当你第一次通过SSH连接到某个主机时，该主机的公钥会被添加到这个文件中。之后，每次连接时，SSH客户端都会检查这个文件，以确保你连接的是正确的主机（防止中间人攻击）。

74/75破解方法

在汇编指令中，相等则跳转机器码74，不相等则跳转机器码75。在破解中常将74换成75，比如在输入密码是，可能是判断密码正确就跳转74，但是我们输入的都猜不对，就会顺序执行到错误的出口，如果我们改成跳转74，那么输入一个错误密码就能跳转到正确出口，登录成功。

ALSR

ALSR（Address Space Layout Randomization）是一种安全机制，用于增加攻击者利用内存中的漏洞来执行恶意代码的难度。它通过随机化进程地址空间中的关键数据结构（如堆、栈、库等）的布局来实现。这样，即使攻击者知道某个漏洞的存在，他们也难以预测和利用该漏洞，因为每次进程运行时，这些关键数据结构的地址都会有所不同。

botnet

僵尸网络 Botnet 是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。在这个网络中，黑客作为控制者，通过特定的控制协议（如IRC协议）与被感染的主机（僵尸主机）进行通信，远程控制这些主机执行恶意任务。

Botnet可以被用于多种攻击，常见的有DDos，发送垃圾邮件等。

chmod

chmod是Unix和类Unix操作系统中的一个命令，用于更改文件或目录的权限。该命令允许用户定义文件或目录的读、写和执行权限，以及文件的所有者、所属组和其他用户的权限

cmd5.com

一个在线MD5加密解密服务网站。cmd5.com 提供了以下服务：

MD5加密： 用户可以在该网站上输入文本，然后网站将生成该文本的MD5哈希值。

MD5解密： 用户可以输入已知的MD5哈希值，然后网站将尝试返回对应的原始文本。这一点有一定的局限性，因为MD5是一种不可逆的哈希函数，但该网站可能通过查找已知的MD5值和其对应的原始文本的数据库来提供服务。

cookie

Cookie机制指的是在浏览网页的时候，服务器将你的登录信息，浏览信息等发送给客户端并保存一段时间，下次访问时可以读取上一次的记录。

CreateRemoteThread()

创建在另一个进程的虚拟地址空间中运行的线程，DDL注入后往往拥有另一个进程的访问权限，此时可以通过该函数攻击。

CTF

中文一般翻译为夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF有答题与攻防两种形式，答题一般有六个方向：MISC, WEB, PWN, REVERSE, CRYPTO,MOBILE。

curl

curl 是一个用于在命令行下进行数据传输的工具和库。它支持许多协议，包括HTTP、HTTPS、FTP、FTPS、SCP、SFTP等。curl 可以用于从或向服务器传输数据，支持各种不同的操作和选项。

DDOS

分布式拒绝服务攻击，DDOS攻击将多个计算机联合起来作为攻击平台，对一个或者多个目标发动攻击，从而成倍的提高拒绝服务攻击的威力。通过大量的请求占用大量网络资源，达到网络瘫痪的目的。

DEP

DEP - 数据执行保护的缩写，Data Execution Prevention。 他是一套软硬件技术，能够在内存上执行额外检查以帮助防止在系统上运行恶意代码。其基本原理是将数据所在内存页标识为不可执行，当程序溢出成功转入shellcode时，程序会尝试在数据页面上执行指令，此时CPU就会抛出异常，而不是去执行恶意指令。
DEP 的主要作用是阻止数据页(如默认的堆页、各种堆栈页以及内存池页)执行代码。微软从 Windows XP SP2开始提供这种技术支持，根据实现的机制不同可分为：软件DEP(Software DEP)和硬件DEP(Hardware-enforced DEP)。

dex2jar

将dex文件转换为包含class文件的jar文件，反编译的逆向工程，不一定成功。

DLL Inject

DLL注入技术，向一个正在运行的进程注入代码的过程，注入的代码以动态链接库（DLL）的形式存在。被注入的动态链接库可以利用它所在的进程权限执行一些特殊任务，比如修改进程内存中的数据，劫持进程的执行流程，监控进程的行为。

DllMain()

DLL（Dynamic Linked Library动态链接库）被加载到进程后会自动运行DllMain()函数，用户可以把想执行的代码放到DllMain()函数，每当加载DLL时，添加的代码就会自然而然得到执行。

DLP

Data Leak Prevention，数据防泄漏工具。有时候数据泄露来自于团队内部成员，比如团队成员利用权限进行拖库操作，DLP相关工具可以防止类似情况发生。该工具普及不多，主要依靠制度防范数据泄露，常见软件有OpenDLP与MyDLP等。

docker

Docker 是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的镜像中，然后发布到任何流行的 Linux或Windows操作系统的机器上，也可以实现虚拟化。容器是完全使用沙箱机制【安全】，相互之间不会有任何接口。

Docker Compose是一个用来定义和运行复杂应用的Docker工具。一个使用Docker容器的应用，通常由多个容器组成。Docker Compose根据配置文件来构建镜像，并使用docker-compose脚本来启动，停止和重启应用，和应用中的服务以及所有依赖服务的容器，非常适合组合使用多个容器进行开发的场景。

DRM

Digital Right Management 数字版权管理，目前对网络中传播的数字作品进行版权保护的主要控制手段。DRM是由美国出版商协会定义的，在数字内容交易过程中对知识产权进行保护的技术，工具和处理过程。

基本的工作原理为：利用秘钥将音频、视频等文件进行加密的编码处理，再建立一个证书授权服务中心，加密的数字节目头部存放着key IP和节目授权中心的URL，当用户使用加密文件时，应用软件会根据其包含在头文件中的有关属性自动链接到相应站点获取相应证书。

GDPR

General Data Protection Regulation 通用数据保护条例，在欧盟法律中对所有欧盟个人关于数据保护和隐私的规范，涉及了欧盟境外的个人资料出口。违反GDPR将面临高额罚款，GDPR也是以重罚为手段，试图倒逼企业完善个人数据保护的制度。

git

Git是一个开源的分布式版本控制系统，可以有效、高速地处理从很小到非常大的项目版本管理。

heartbeat

通过HeartBeat，可以将资源（IP以及程序服务等资源）从一台已经故障的计算机快速转移到另一台正常运转的机器上继续提供服务，一般称之为高可用的服务。

HeartBeat的工作原理：通过修改Heartbeat的软件的配置文件，可以制定那一台Heartbeat服务器作为主服务器，则另一台将自动成为热备服务器。然后在热备服务器上配置Heartbeat守护程序来监听来自主服务器的心跳消息。如果热备服务器在指定时间内为监听到来自主服务器的心跳，就会启动故障转移程序，并取得主服务器上的相关资源服务的所有权，接替主服务器继续不间断的提供服务，从而达到资源以及服务高可用的目的。

heartbleed

heartbleed 漏洞的产生是由于未能在memcpy( )调用受害用户输入内容作为长度参数之前正确进行边界检查。攻击者可以追踪OpenSSL所分配的64KB缓存，将超出必要范围的字节信息复制到缓存中再返回缓存内容，这样一来受害者的内容就会以64KB的速度进行泄露。

此问题的原因是在实现TLS的心跳扩展时没有对输入进行适当验证，因此漏洞名称为heartbleed 。

honeypot

蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主句、网络服务或者信息，诱导攻击方对它们实施攻击。从而可以通过对攻击行为进行捕获和分析，了解攻击方所使用的的工具与方法，推测攻击意图和动机，能够让防御方清晰的了解它们所面对的安全威胁，并且通过技术和管理手段来增强实际系统的安全防护能力。

蜜罐更像是一个情报收集系统，提供一个安全的被攻击环境，以此来收集服务器是怎么被攻击的等信息，还可以通过窃听黑客之间的联系，收集黑客用的工具吗，掌握他们的社交网络。

HTTPS

HTTP是明文传输，所以会很有可能产生中间人攻击，HTTPS加密应运而生。

为了解决这个安全问题，HTTPS在HTTP基础上添加了一层安全套接层(SSL)或传输层安全性(TSL)协议，这个安全层使用加密算法保护数据传输，确保在浏览器和服务器之间的通信是安全的和私密的。

ICAP

Internet Content Adaptation Protocol（互联网内容适配协议）的缩写，是一种用于在网络流量中应用内容适应和修改的协议，主要目的是允许网络中的设备通过外部服务对传输内容进行修改、适应、审查。

它在本质上是在HTTP message上执行RPC远程过程调用的一种轻量级的协议, 也就是说, 它让ICAP Client可以把HTTP Message传给ICAP Server，然后ICAP Server可以对其进行某种变换或者其他处理(“匹配”).被变换的message可以是HTTP请求也可以是HTTP应答.

IDApro

IDA Pro是一款功能强大的反汇编和逆向工程工具，通过其深度分析能力、强大的自动化支持和广泛的插件扩展，满足了多种复杂的安全研究和逆向工程需求。

IDA Pro能够创建执行映射以显示二进制文件，并以符号表示形式展示处理器执行的指令（程序集）语言。

iptables

iptables 是集成在 Linux 内核中的包过滤防火墙系统，是 Linux 防火墙系统的重要组成部分。

iptables 的主要功能是实现对网络数据包进出设备及转发的控制。当数据包需要进入设备、从设备中流出或者由该设备转发、路由时，都可以使用 iptables 进行控制。

Kerberos

Kerberos是一个网络身份验证协议，它提供了一种安全的身份验证机制，允许在不安全的网络上的用户和服务进行安全通信。步骤如下：

认证请求： 用户向Kerberos认证服务器请求认证，提供自己的身份信息。

票据颁发： Kerberos服务器验证用户身份，并生成一个加密的票据（Ticket）。这个票据包含有关用户身份和授权信息的加密信息。
票据传递： 用户向需要验证身份的服务发出请求，同时提供由Kerberos服务器颁发的票据。
票据验证： 服务使用共享密钥与Kerberos服务器共同解密票据，验证用户的身份和授权信息。
会话建立： 一旦票据被验证，服务和用户之间建立一个安全的会话，允许双方进行安全通信。

Metasploit

MetaSploit Framework是一个开源的渗透测试框架，提供了一组工具和模块，用于网络安全测试、漏洞利用和渗透测试。附带数千个已知的软件漏洞，并保持持续更新。Metasploit可以用来信息收集、漏洞探测、漏洞利用等渗透测试的全流程，被安全社区冠以“可以黑掉整个宇宙”之名。

mydlp

DLP Data Loss Prevention，数据防泄漏工具。有时候数据泄露来自于团队的内部成员，比如团队成员利用权限进行拖库操作，DLP相关工具可以防止类似情况的发生。该类工具普及不多，主要依靠制度防范数据内部泄露，常见软件有OpenDLP和MyDLP等。

NAS

Network Attached Storage 网络附加存储，一种专门用于数据存储和共享的设备，通过网络连接提供文件服务。NAS通常是一个独立的硬件设备，也可以是一个运行特定NAS软件的服务器，主要目的是通过网络提供文件访问服务，让多个用户可以方便地共享和访问存储在其中的数据。

nmap

Network Mapper 是一个网络扫描和主机发现工具，可以用来查找网络上的主机、服务和操作系统信息。Nmap可以扫描整个网络或单个主机，并且可以生成详细报告。还可以用于安全评估，帮助识别未修补漏洞和其他安全问题。

ntop/ntopng

ntopng：ntop next generation是一个开源网络流量监测工具，可以收集、分析、报告网络流量数据，包括IP协议分布、主机流量、应用程序流量等，ntopng还可以用于监测和诊断网络性能问题，提供了web界面和API访问监测数据。

O-LLVM

Obfuscator-LLVM基于LLVM的代码混淆工具，代码混淆工具是一种用于混淆源代码以防止反编译的工具。使用各种技术更改代码的结构和语法，使其难以被阅读或理解，一些常用的混淆技术包括重命名变量和函数、添加无用代码、更改代码流程等。

ollydbg

ollydbg常被称为OD,又被称作OllyDebug，是一个常用的反汇编工具，目前最流行的调试解密工具，还支持插件扩展功能

PAP

两次握手认证，通过链路建立阶段协商的认证方式进行链路认证

第一次握手，被认证方将配置的用户名和密码信息以明文方式发送给认证方

第二次握手，认证方收到被认证方发送的用户名和密码信息之后，根据本地配置的用户名和密码数据库检查用户名和密码信息是否匹配，如果匹配的话则返回ACK报文，表示认证成功。否则返回NAK报文表示认证失败。

Phishing

钓鱼是一种网络欺诈手段，目的是通过欺骗和诱导用户提供个人敏感信息，如用户名、密码、信用卡号等。攻击者通常伪装成可信赖的实体，如银行、电子邮件服务提供商、社交媒体平台等，以欺骗用户相信他们正在与合法实体进行通信。

PKCS#11

PKCS#11是密码学标准的一部分，全称Public Key Crytography Standard #11，定义了一个应用程序编程接口API，用于在安全硬件设备中执行加密操作、签名和秘钥管理等安全功能。

RADIUS

Remote Authentication Dial-In User Service 远程身份验证拨号用户服务，是一种广泛用于网络访问控制和身份验证的协议。最初设计用于拨号用户通过拨号接入服务进行身份验证，后来也被用于其他类型的网络访问，如无线局域网、虚拟专用网络等。

RADIUS协议主要功能包括，身份验证、授权、计费。

robots.txt

一种用于网站管理的标准，运行网站管理员指导网络爬虫哪些页面可以被爬取，哪些页面应该被忽略。这个文件通常放在根目录下，由搜索引擎蜘蛛在抓取网站内容之前查看。

rust

一种系统编程语言，强调安全性、并发性和性能。设计的目标是提供一种能够避免常见的内存安全错误的语言，同时保持高性能和高并发。被广泛应用于系统级编程、嵌入式开发、网络服务等需要高性能和安全性的应用领域，其独特设计和强大功能使其成为一个备受欢迎的编程软件。

SGX

Software Guard Extensions 软件保护扩展，是Intel推出的一种硬件级别的安全技术，主要目标是提供一种安全的执行环境，使得敏感数据和代码在计算机上运行时可以受到保护。

主要特点如下：

使用安全的执行环境使应用程序在受保护的区域内运行
通过硬件隔离，使得敏感数据在enclave内部得到保护，防止恶意软件或其他应用程序访问这些数据
还可以用于保护应用程序的关键代码片段，防止非授权的代码修改
提供一种可信计算的机制，使得计算过程可以被验证，并且能在运行时保护敏感信息

shadowsocks

shadowsocks是一种网络代理工具，它使用自定义协议来隐藏用户的互联网流量，绕过防火墙和地域限制，使用加密保护用户隐私，可以在各种平台上使用。

shadowsocksR：SSR，使用更高级的加密方式，支持更多协议。

Shellcode

缓冲区溢出的常用攻击方法，使用shellcode地址覆盖漏洞程序的返回地址，使得漏洞程序去执行存放在栈中的shellcode。为了阻止这种类型的攻击，一些操作系统使得系统管理员具有使栈不可执行的能力。

socat

是一个用于在UNIX系统中建立连接的命令行工具，可以创建两个数据流之间的连接。主要用于处理套接字，应用于多种任务，包括网络调试、端口重定向、加密通信、代理等。其强大之处在于它的灵活性和可配置性，支持多种协议、地址族、及数据传输方式，可以解决各种网络和系统编程任务。

sql注入

SQL注入是一种网络安全漏洞，允许攻击者通过在应用程序的输入中插入恶意的SQL代码，从而执行未经授权的数据库操作，这种攻击常常发生在与数据库交互的web程序中，其中用户提供的输入未经适当验证与处理，导致恶意SQL代码被执行。

ssh -D

ssh -D 是使用SSH命令的一个选项，用于创建动态端口转发，也称为SOCKS代理，这个选项允许通过安全的SSH连接，将本地计算机上的数据转发到远程服务器，并且可以通过这个服务器访问互联网。

在使用 ssh -D 后，你可以配置本地计算机上的应用程序，比如浏览器或其他网络工具，以使用创建的 SOCKS 代理。这样，所有通过该应用程序发出的网络请求都将通过 SSH 连接路由到远程服务器，并由远程服务器发起。这提供了一种安全的方式，特别适用于在不受信任的网络上浏览互联网或访问受限制的资源。

ssh -L

SSH -L (Local Port Forwarding) 是一种 SSH 的功能，它允许将本地计算机上的某个端口连接到远程计算机上的另一个端口上。这样做可以通过远程计算机来访问本地计算机上的资源，例如数据库或 Web 服务器。

ssh -R

SSH -R (Remote Port Forwarding) 是另一种 SSH 的功能，它允许将远程计算机上的某个端口连接到本地计算机上的另一个端口上。这样做可以通过本地计算机来访问远程计算机上的资源，例如远程数据库或 Web 服务器。

SSO

Single Sign-On 单点登录，一种身份验证和授权机制，允许用户使用一组凭证登录到多个相关但是独立的软件系统或应用程序中，无需为每个系统单独进行身份验证。SSO的主要目标是提供用户友好的身份验证体验，同时减轻用户对多个系统和服务进行独立登录的负担。具体来说，当用户成功登录到一个系统后，他们无需再次输入凭证就可以访问其他受信任的系统，因为这些系统之间实现了共享的身份验证信息。

SYN flood

TCP-SYN Flood攻击又称半开式连接攻击，每当我们进行一次标准的TCP连接，都会有一个三次握手的过程，而TCP-SYN Flood在它的实现过程中只有前两个步骤。这样，服务方会在一定时间内处于等待接收请求方ACK消息的状态。由于一台服务器可用的TCP连接是有限的，如果恶意攻击方快速连续的发送此类连接请求，则服务器可用的TCP连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常网络服务，从而造成拒绝服务。

tcpdump

tcpdump是一个在UNIX/LINUX系统上用于捕获网络数据包的命令行工具，可以监听网络接口，显示经过该接口的数据包的详细信息，包括源地址、目的地址、协议、端口等信息。tcpdump对于网络故障的排除、网络分析和安全审计等任务非常有用。

TOR

匿名网络。TOR用户在本机运行一个洋葱代理服务器（onion proxy），这个代理器周期的与其他TOR交流。其中每个路由器的传输都经过对等秘钥来加密，形成具有层次的结构。进入TOR网络后，加密信息在路由器间层层传递，最后到达出口节点，明文数据从这个节点直接发往原来目的地。对于目的主机而言是从出口节点发来信息，要注意的是明文信息即使在TOR网络中是加密的，离开TOR后仍然是明文的。

VNC

Virtual Network Computing是一种远程桌面协议，允许用户远距离查看和控制另一台计算机上的桌面。VNC通过网络将远程计算机的屏幕和键盘/鼠标输入传送到本地计算机，从而使用户可以在本地计算机上远程操作。

vulhub

开源的漏洞靶场项目，可以帮助安全研究人员和渗透测试人员研究和模拟各种漏洞攻击，提供了常见系统和应用的虚拟机镜像。

提供了详细的安装和配置说明，可以帮助用户快速搭建漏洞攻击环境，vulhub还提供了漏洞攻击的详细描述和利用方法，帮助用户更好的理解和模拟漏洞攻击。此外vulhub还支持在Docker中运行，为研究人员和安全工程师提供更快捷的漏洞环境。

wget

是一个用于从web上下载文件的命令工具，支持HTTP、HTTPS和FTP协议下载文件，是许多UNIX/LINUX系统中的常用工具之一。wget提供了许多选项，用于控制下载过程的各个方面。

whois

读作who is，用来查询域名的IP以及所有者等信息的传输协议。简单来说whois就是一个用来查询域名是否已经被注册，以及注册名的详细信息的数据库。

Windows更新服务

WSUS(windows server update services)是微软提供的用于管理windows更新的服务，可以让管理员在本地部署一个更新服务器，以便更新组织内的windows计算机，便于管理员进行windows更新补丁管理。WSUS可以通过下载微软的更新补丁，并将其分发到组织内的计算机来提高windows系统的安全性、稳定性。

网络攻防中，WSUS可以帮助防止攻击者利用已知漏洞进入网络，通过使用WSUS，管理员可以确保所有客户端都安装了最新的安全更新，降低被攻击的风险。

Wireshark

Wireshark是一个网络封包分析软件，网络封包分析软件的功能是截取网络封包，并尽可能显示出最详细的网络封包资料。使用winPCAP作为接口，直接与网卡进行数据报文交换。

WriteProcessMemory()

WriteProcessMemory是C++中的函数，可以写入某一进程的内存区域，直接写入会出现Access violation错误，因此需要此函数入口区必须可以访问，否则将操作失败。

x64dbg

x64dbg 是一款开源的、目前仍在积极开发中的 x32/x64 位动态调试器。其界面及操作方法与 OllyDbg 类似，和 OllyDbg 不同的是它可以对 64 位程序进行调试。此外，其开放式的设计给了此软件很强的生命力。通过爱好者们不断的修改和扩充，使其功能越来越强大。

x64dbg 是逆向工程师的常用工具之一，可以用来调试目标程序，分析恶意软件、逆向工程和代码审计。同时也可以帮助软件开发人员调试代码，查找并修复错误。

XKMS

XML key Management Specification 是一种用于在计算机网络上管理和分发公钥和其他安全令牌的标准，旨在提供一种标准化的方式，使应用程序能够通过XML协议进行密钥管理操作。总的来说，XKMS通过标准化密钥管理服务，使得安全性的实现更加便捷，支持在不同应用和系统之间共享和管理安全令牌。

XSS

跨站脚本攻击，允许攻击者在不被授权的情况下将恶意代码注入到网页中，影响到访问该网页的用户。攻击者可以利用XSS漏洞来窃取用户的私人信息，也可以改变网站的外观和行为，以欺骗用户。

往年CSDN