走向大神之路 II

IT 萌新必知の技术黑话

攻击篇			防守篇	
攻击工具	41、鱼叉攻击、	76、白帽黑客	115 沙箱逃逸	157、元数据
1、肉鸡	42、钓鲸攻击	77、红帽黑客	116、网络靶场	158、欺骗检测
2、僵尸网络	43、水坑攻击	78、红队	防守技术与服务	159、微隔离
3、木马	44、嗅探	79、蓝队	117、加密技术	160、逆向
4、网页木马	45、APT 攻击	80 紫队	118、黑名单	161、无代理安全
5、Rootkit	46、C2		119、白名单	162、CWPP
6、蠕虫病毒	47、供应链攻击		120、内网	163、CSPM
7、震网病毒	48、社会工程学	防守软硬件	121、外网	164、CASB
8、勒索病毒	49、黑客技术	81、加密机	122、边界防御	165、防爬
9、挖矿木马	50、拿站	82、CA 证书	123、南北向流量	166、安全资源池
10、攻击载荷	51、提权	83、SSL 证书	124、东西向流量	167、IAM
11、嗅探器（Sniffer）	52、渗透	84、防火墙	125、规则库	168、4A
12、恶意软件	53、横移	85、IDS	126、下一代	169、ACL
13、间谍软件	54、跳板	86、NIDS	127、大数据安全分析	170、多因子认证
14、后门	55、网马	87、IPS	128、EPP	171、特权账户管理
15、弱口令	56、黑页	88、杀毒软件	129、EDP	172、零信任
16、漏洞	57、暗链	89、反病毒引擎	130、NDR	173、SDP
17、远程命令执行漏洞	58、拖库	90、防毒墙	131、安全可视化	174、SAAS
18、0day 漏洞	59、撞库	91、老三样	132、NTA	175、同态加密
19、1day 漏洞	60、暴库	92、告警	133、MDR	176、量子计算
20、Nday 漏洞	61、CC 攻击	93、误报	134、应急响应	177、可信计算
攻击方法	62、Webshell	94、漏报	135、XDR	178、拟态防御
21、挂马	63、跨站攻击	95、NAC	136、安全运营	179、区块链
22、挖洞	64、中间人攻击	96、漏扫	137、威胁情报	180、远程浏览器
23、加壳	65、薅羊毛	97、UTM	138、TTP	181、云手机
24、溢出	66、BEC	98、网闸	139、IOC	182、风控
25、缓冲区溢出	67、电信诈骗	99、堡垒机	140、上下文	183、渗透测试
26、注入	68、杀猪盘	100、数据库审计	141、STIX	184、安全众测
27、SQL 注入	69、ARP 攻击	101、DLP	142、杀伤链	185、内生安全
28、注入点	70、欺骗攻击	102、VPN	143、ATT&CK	186、内生安全框架
29、软件脱壳	71、Shellcode	103、SD-WAN	144、钻石模型	187、PPDR
30、免杀	72、物理攻击	104、云服务	145、关联分析	188、CARTA
31、暴力破解	67、电信诈骗	105、路由器	146、态势感知	189、SASE
32、洪水攻击	68、杀猪盘	106、网关	147、探针	190、SDL
33、SYN 攻击	69、ARP 攻击	107、WAF	148、网络空间测绘	191、DevOps
34、DoS 攻击	70、欺骗攻击	108、SOC	149、SOAR	192、代码审计
35、DDoS	71、Shellcode	109、LAS	150、UEBA	193、NTLM 验证
36、抓鸡	72、物理攻击	110、NOC	151、内存保护	194、MTTD
37、端口扫描	攻击者	111、SIEM	152、RASP	195、MTTR
38、花指令	73、黑产	112、上网行为管理	153、包检测	196、CVE
39、反弹端口	74、暗网	113、蜜罐	155、深度包检测	197、软件加壳
40、网络钓鱼	75、黑帽黑客	114、沙箱	156、全流量检测	198、CNVD

199、数据脱敏				
200、GDPR				
201、CCPA				
202、SRC				
203、CISO/CSO				
204、IPC 管道				
205、SYN 包				
206、IPC$				
207、shell				
208、ARP				

攻击篇

一、攻击工具

1、肉鸡
“肉鸡”也成为傀儡机，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，黑客可以随意操纵它并利用它做任何事情， 肉鸡通常被用作 DDOS 攻击，也常常会被作为攻击跳板。
例如在 2016 年美国东海岸断网事件中，黑客组织控制了大量的联网摄像头用于发动网络攻击，这些摄像头则可被称为“肉鸡”。

2、僵尸网络
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。
僵尸网络是一个非常形象的比喻，众多的计算机在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被攻击者执行各类恶意活动（DDOS、垃圾邮件等）利用的一种基础设施。

3、木马
“木马”这一名称来源于希腊神话特洛伊战争的特洛伊木马。就是那些表面上伪装成了正常的程序，但是当这些程序运行时，就会获取系统的整个控制权限。

网络安全领域的木马是一种有害的程序，其特征与特洛伊木马一样具有伪装性，表面上没有危害、甚至还附有用户需要的功能。有很多黑客就是热衷使用木马程序来控制别人的电脑，比如灰鸽子、GhOst、PcShare 等等。
木马

但用户一旦运行，就会对产生破坏或窃取数据，特别是用户的各种账户及口令等重要且需要保密的信息，甚至控制用户的计算机系统。

4、网页木马
表面上伪装成普通的网页或是将恶意代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马服务端植入到访问者的电脑上来自动执行将受影响的客户电脑变成肉鸡或纳入僵尸网络。

5、Rootkit
Rootkit 是攻击者用来隐藏自己的行踪和保留 root（根权限，可以理解成 WINDOWS 下的 system 或者管理员权限）访问权限的工具。
通常，攻击者通过远程攻击的方式获得 root 访问权限，或者是先使用密码猜解（破解）的方式获得对系统的普通访问权限，进入系统后，再通过对方系统存在的安全漏洞获得系统的 root 或 system 权限。

然后，攻击者就会在对方的系统中安装 Rootkit，以达到自己长久控制对方的目的，Rootkit 功能上与木马和后门很类似，但远比它们要隐蔽。

6、蠕虫病毒
它是一类相对独立的恶意代码，利用了联网系统的开放性特点，通过可远程利用的漏洞自主地进行传播，受到控制终端会变成攻击的发起方，尝试感染更多的系统。蠕虫病毒的主要特性有：自我复制能力、很强的传播性、潜伏性、特定的触发性、很大的破坏性。

蠕虫是一种可以自我复制的代码，并且通过网络传播，通常无需人为干预就能传播，受到控制终端会变成攻击的发起方，尝试感染更多的系统。蠕虫通常基于垃圾邮件和漏洞利用这两种方法来进行传播。

计算机发展史上著名的冲击波、震荡波、熊猫烧香、永恒之蓝，都属于蠕虫病毒。

7、震网病毒
又名 Stuxnet 病毒，是第一个专门定向攻击真实世界中基础（能源）设施的“蠕虫”病毒，比如核电站，水坝，国家电网。
作为世界上首个网络“超级破坏性武器”，Stuxnet 的计算机病毒已经感染了全球超过 45000 个网络，其目标伊朗的铀浓缩设备遭到的攻击最为严重。

8、勒索病毒
勒索病毒其实是蠕虫病毒的一种，但相比普通蠕虫主要消耗网络带宽、拖慢系统而言，勒索病毒是目前危害最大的一种蠕虫，一旦感染将给用户带来无法估量的损失。

主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。

这种病毒通常利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。而黑客就可以以此来进行勒索敲诈。
最著名的勒索病毒是永恒之蓝（wannacry）。

9、挖矿木马
一种将 PC、移动设备甚至服务器变为矿机的木马，通常由挖矿团伙植入，用于挖掘比特币从而赚取利益。

10、攻击载荷
攻击载荷（Payload）是系统被攻陷后执行的多阶段恶意代码。
通常攻击载荷附加于漏洞攻击模块之上，随漏洞攻击一起分发，并可能通过网络获取更多的组件。

11、嗅探器（Sniffer）
就是能够捕获网络报文的设备或程序。嗅探器的正当用处在于分析网络的流量，以便找出所关心的网络中潜在的问题。

12、恶意软件
被设计来达到非授权控制计算机或窃取计算机数据等多种恶意行为的程序。

13、间谍软件
一种能够在用户不知情的情况下，在其电脑、手机上安装后门，具备收集用户信息、监听、偷拍等功能的软件。

14、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，就好象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。

很多时候，后门是开发者为了方便自己维护和调试，而预先设置好的。比如超级口令，或者隐藏的路径。也可能是入侵者在获得系统控制权后，悄悄设置的。

后门与传统病毒不同，它自身并没有传染性（自我复制性），但很多病毒在感染系统后，会悄悄植入后门。

通常大多数木马程序都可以被入侵者用于创建后门（BackDoor）。
15、弱口令
指那些强度不够，容易被猜解的，类似 123，abc 这样的口令（密码）。

16、漏洞
漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，IT 资产中能被威胁所利用的弱点。从而可以使攻击者能够在未授权的情况下访问或破坏系统。使得系统或其应用数据的保密性、完整性、可用性、访问控制等面临威胁。

软件的缺陷是漏洞的一个主要来源，缺陷是天生的，漏洞是不可避免的。

\最知名的是“0 day”漏洞，通常是指在系统商在知晓并发布相关补丁前就被掌握或者公开的漏洞信息。

零日漏洞不但是黑客的最爱，掌握多少零日漏洞也成为评价黑客技术水平的一个重要参数

17、远程命令执行漏洞
由于系统设计实现上存在的漏洞，攻击者可能通过发送特定的请求或数据导致在受影响的系统上执行攻击者指定的任意命令。

18、0day 漏洞
0day 漏洞最早的破解是专门针对软件的，叫做 WAREZ，后来才发展到游戏，音乐，影视等其他内容的。
0day 中的 0 表示 Zero，早期的 0day 表示在软件发行后的 24 小时内就出现破解版本。

在网络攻防的语境下，0day 漏洞指那些已经被攻击者发现掌握并开始利用，但还没有被包括受影响软件厂商在内的公众所知的漏洞，这类漏洞对攻击者来说有完全的信息优势，由于没有漏洞的对应的补丁或临时解决方案，防守方不知道如何防御，攻击者可以达成最大可能的威胁。

19、1day 漏洞
指漏洞信息已公开但仍未发布补丁的漏洞。此类漏洞的危害仍然较高，但往往官方会公布部分缓解措施，如关闭部分端口或者服务等。

20、Nday 漏洞
指已经发布官方补丁的漏洞。通常情况下，此类漏洞的防护只需更新补丁即可，但由于多种原因，导致往往存在大量设备漏洞补丁更新不及时，且漏洞利用方式已经在互联网公开，往往此类漏洞是黑客最常使用的漏洞。
例如在永恒之蓝事件中，微软事先已经发布补丁，但仍有大量用户中招。

2、攻击方法

21、挂马
就是在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

22、挖洞
指漏洞挖掘。

23、加壳
就是利用特殊的算法，将 EXE 可执行程序或者 DLL 动态连接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX，ASPack、PePack、PECompact、UPack、免疫 007、木马彩衣等等。

24、溢出
简单的解释就是程序对输入数据没有执行有效的边界检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。

25、缓冲区溢出
攻击者向一个地址区输入这个区间存储不下的大量字符。在某些情况下，这些多余的字符可以作为“执行代码”来运行，因此足以使攻击者不受安全措施限制而获得计算机的控制权。

26、注入
Web 安全头号大敌。攻击者把一些包含攻击代码当做命令或者查询语句发送给解释器，这些恶意数据可以欺骗解释器，从而执行计划外的命令或者未授权访问数据。
注入攻击漏洞往往是应用程序缺少对输入进行安全性检查所引起的。注入漏洞通常能在 SQL 查询、LDAP 查询、OS 命令、程序参数等中出现。

27、SQL 注入
注入攻击最常见的形式，主要是指 Web 应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在 Web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询或其他操作，导致数据库信息泄露或非授权操作数据表。

28、注入点
即可以实行注入的地方，通常是一个涉及访问数据库的应用链接。根据注入点数据库的运行帐号的权限的不同，你所得到的权限也不同。

29、软件脱壳
顾名思义，就是利用相应的工具，把在软件“外面”起保护作用的“壳”程序去除，还文件本来面目，这样再修改文件内容或进行分析检测就容易多了。

30、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。

31、暴力破解
简称“爆破”。黑客对系统中账号的每一个可能的密码进行高度密集的自动搜索，从而破坏安全并获得对计算机的访问权限。

32、洪水攻击
是黑客比较常用的一种攻击技术，特点是实施简单，威力巨大，大多是无视防御的。
从定义上说，攻击者对网络资源发送过量数据时就发生了洪水攻击，这个网络资源可以是 router，switch，host，application 等。
洪水攻击将攻击流量比作成洪水，只要攻击流量足够大，就可以将防御手段打穿。
DDoS 攻击便是洪水攻击的一种。

33、SYN 攻击
利用操作系统 TCP 协调设计上的问题执行的拒绝服务攻击，涉及 TCP 建立连接时三次握手的设计。

34、DoS 攻击
拒绝服务攻击。拒绝服务攻击（DoS）是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问,攻击者通过利用漏洞或发送大量的请求导致攻击对象无法访问网络或者网站无法被访问。

35、DDoS
分布式 DOS 攻击，常见的 UDP、SYN、反射放大攻击等等，就是通过许多台肉鸡一起向你发送一些网络请求信息，导致你的网络堵塞而不能正常上网。

当黑客使用网络上两个或以上被攻陷的电脑作为“僵尸”向特定的目标发动“拒绝服务”式

攻击时，称为分布式拒绝服务攻击。

曾经，DDoS 最流行的领域，是网游私服，不同的私服经营者之间，进行“互 D”，用 DDoS 把友商的私服搞瘫，自家的生意就更火。

36、抓鸡
即设法控制电脑，将其沦为肉鸡。

37、端口扫描
端口扫描是指发送一组端口扫描消息，通过它了解到从哪里可探寻到攻击弱点，并了解其提供的计算机网络服务类型，试图以此侵入某台计算机。

38、花指令
通过加入不影响程序功能的多余汇编指令，使得杀毒软件不能正常的判断病毒文件的构造。说通俗点就是“杀毒软件是从头到脚按顺序来识别病毒。如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了”。

39、反弹端口
有人发现，防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范。
于是，利用这一特性，反弹端口型软件的服务端(被控制端)会主动连接客户端(控制端)，就给人“被控制端主动连接控制端的假象，让人麻痹大意。

40、网络钓鱼
攻击者利用欺骗性的电子邮件或伪造的 Web 站点等来进行网络诈骗活动。
诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息或邮件账号口令。
受骗者往往会泄露自己的邮箱、私人资料，如信用卡号、银行卡账户、身份证号等内容。

41、鱼叉攻击
鱼叉攻击是将用鱼叉捕鱼形象的引入到了网络攻击中，鱼叉攻击又称为「鱼叉式」网络钓鱼，主要是指可以使欺骗性电子邮件看起来更加可信的网络钓鱼攻击，具有更高的成功可能性。

不同于撒网式的网络钓鱼，鱼叉攻击往往更加具备针对性，攻击者往往“见鱼而使叉”。
为了实现这一目标，攻击者将尝试在目标上收集尽可能多的信息。通常，组织内的特定个人存在某些安全漏洞。

鱼叉式网络钓鱼锁定的对象并非普通个人，而是特定公司、组织的成员，因此被窃取的资料也不是普通网络钓鱼所窃取的个人资料，而是高度敏感性资料，如知识产权及商业机密。

42、钓鲸攻击
捕鲸是另一种进化形式的鱼叉式网络钓鱼。比鱼叉更进一步，锁定更重要的目标，通常针对高级管理人员和组织内其他高级人员，钓鱼就钓大鱼。它指的是针对高级管理人员和组织内其他高级人员的网络钓鱼攻击。

通过使电子邮件内容具有个性化并专门针对相关目标进行定制的攻击。

通过使电子邮件内容具有个性化并专门针对相关目标进行定制的攻击。

43、水坑攻击
顾名思义，是在受害者必经之路设置了一个“水坑(陷阱)”。 让受害者掉坑。

与「鱼叉」和「钓鲸」直接攻击目标对象不同，水坑采用了一种间接方法：攻击者首先分析目标人群经常访问的网站，然后入侵其中一个或多个网站，植入恶意软件，此时，一旦攻击目标访问该网站就会“中招”。

水坑攻击借助了目标组织所信任的网站，攻击成功率很高，即便是那些对鱼叉攻击或其他形式的网络钓鱼具有防护能力的组织，都可能不慎“入坑”。

44、嗅探
嗅探指的是对局域网中的数据包进行截取及分析，从中获取有效信息。

45、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。通常是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为，是一种蓄谋已久的“恶意商业间谍威胁”

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。

这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。APT 的攻击手法，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据。

APT 并不是单一攻击行为，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。

46、C2
C2 全称为 Command and Control，命令与控制，常见于 APT 攻击场景中。作动词解释时理解为恶意软件与攻击者进行交互，作名词解释时理解为攻击者的“基础设施”。

47、供应链攻击
是黑客攻击目标机构的合作伙伴，并以该合作伙为跳板，达到渗透目标用户的目的。
一种常见的表现形式为，用户对厂商产品的信任，在厂商产品下载安装或者更新时进行恶意软件植入进行攻击。
所以，在某些软件下载平台下载的时候，若遭遇捆绑软件，就得小心了！

48、社会工程学
一种无需依托任何黑客软件，更注重研究人性弱点的黑客手法正在兴起，这就是社会工程学

49、黑客技术。
通俗而言是指利用人的社会学弱点实施网络攻击的一整套方法论，其攻击手法往往出乎人意料。
世界第一黑客凯文·米特尼克在《反欺骗的艺术》中曾提到，人为因素才是安全的软肋。很多企业、公司在信息安全上投入大量的资金，最终导致数据泄露的原因，往往却是发生在人本身。

50、拿站
指得到一个网站的最高权限，即得到后台和管理员名字和密码。

51、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。

52、渗透
就是通过扫描检测你的网络设备及系统有没有安全漏洞，有的话就可能被入侵，就像一滴水透过一块有漏洞的木板，渗透成功就是系统被入侵。

53、横移
指攻击者入侵后，从立足点在内部网络进行拓展，搜寻控制更多的系统。

54、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。

55、网马
就是在网页中植入木马，当打开网页的时候就运行了木马程序。

56、黑页
黑客攻击成功后，在网站上留下的黑客入侵成功的页面，用于炫耀攻击成果。

57、暗链
看不见的网站链接，“暗链”在网站中的链接做得非常隐蔽，短时间内不易被搜索引擎察觉。它和友情链接有相似之处，可以有效地提高网站权重。

58、拖库
拖库本来是数据库领域的术语，指从数据库中导出数据。
在网络攻击领域，它被用来指网站遭到入侵后，黑客窃取其数据库文件，把库里的数据都“拖”下来。

59、撞库
撞库是指黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。

说的直白点：很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在A网站的账户从而尝试登录B网址，这就是撞库攻击。

60、暴库
入侵网站的一种手法，通过恶意代码让网站爆出其一些敏感数据来。

61、CC攻击
即Challenge Collapsar，名字来源于对抗国内安全厂商绿盟科技早期的抗拒绝服务产品黑洞，攻击者借助代理服务器生成指向受害主机的涉及大量占用系统资源的合法请求，耗尽目标的处理资源，达到拒绝服务的目的。

62、Webshell
Webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做是一种网页后门，可以上传下载文件，查看数据库，执行任意程序命令等。

63、跨站攻击
通常简称为XSS，是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的HTML代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。

64、中间人攻击
中间人攻击是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而这台计算机就称为“中间人”。

65、薅羊毛
指网赚一族利用各种网络金融产品或红包活动推广下线抽成赚钱，又泛指搜集各个银行等金融机构及各类商家的优惠信息，以此实现盈利的目的。这类行为就被称之为薅羊毛。

66、商业电子邮件攻击（BEC）
也被称为“变脸诈骗”攻击，这是针对高层管理人员的攻击，攻击者通常冒充（盗用）决策者的邮件，来下达与资金、利益相关的指令；或者攻击者依赖社会工程学制作电子邮件，说服/诱导高管短时间进行经济交易。

67、电信诈骗
是指通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为，通常以冒充他人及仿冒、伪造各种合法外衣和形式的方式达到欺骗的目的。

68、杀猪盘
网络流行词，电信诈骗的一种，是一种网络交友诱导股票投资、赌博等类型的诈骗方式，“杀猪盘”则是“从业者们”自己起的名字，是指放长线“养猪”诈骗，养得越久，诈骗得越狠。

69、ARP 攻击
ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的进行。
基于 ARP 协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的 ARP 数据包，数据包内包含有与当前设备重复的 Mac 地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。

70、欺骗攻击
网络欺骗的技术主要有：HONEYPOT 和分布式 HONEYPOT、欺骗空间技术等。
主要方式有：IP 欺骗、ARP 欺骗、 DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗（通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作）、地址欺骗（包括伪造源地址和伪造中间站点）等。

71、Shellcode
一段可被操作系统无需特别定位处理的指令，通常在利用软件漏洞后执行的恶意代码，shellcode 为二进制的机器码，因为经常让攻击者获得 shell 而得名。

72、物理攻击
通俗理解，即采用物理接触而非技术手段达到网络入侵的目的，最常见的表现形式为插 U 盘。著名的震网病毒事件即通过插 U 盘的形式，感染了伊朗核设施。

3. 攻击者

73、黑产
网络黑产，指以互联网为媒介，以网络技术为主要手段，为计算机信息系统安全和网络空间管理秩序，甚至国家安全、社会政治稳定带来潜在威胁（重大安全隐患）的非法行为。
例如非法数据交易产业。

74、暗网
暗网是利用加密传输、P2P 对等网络、多点中继混淆等，为用户提供匿名的互联网信息访问的一类技术手段，其最突出的特点就是匿名性。

75、黑帽黑客
以非法目的进行黑客攻击的人，通常是为了经济利益。他们进入安全网络以销毁、赎回、修改或窃取数据，或使网络无法用于授权用户。
这个名字来源于这样一个历史：老式的黑白西部电影中，恶棍很容易被电影观众识别，因为他们戴着黑帽子，而“好人”则戴着白帽子。

76、白帽黑客
是那些用自己的黑客技术来进行合法的安全测试分析的黑客，测试网络和系统的性能来判定它们能够承受入侵的强弱程度。

77、红帽黑客
事实上最为人所接受的说法叫红客。
红帽黑客以正义、道德、进步、强大为宗旨，以热爱祖国、坚持正义、开拓进取为精神支柱，红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击。

77+、绿帽黑客
白天出门给人讲安全 PPT，晚上回家发现自己电脑被黑了，XXX 安全卫士没防住，史称绿帽黑客。

78、红队
通常指攻防演习中的攻击队伍。

79、蓝队
通常指攻防演习中的防守队伍。

80、紫队
攻防演习中新近诞生的一方，通常指监理方或者裁判方。

二、防守篇

1. 软硬件

81、加密机
主机加密设备，加密机和主机之间使用 TCP/IP 协议通信，所以加密机对主机的类型和主机操作系统无任何特殊的要求。

82、CA 证书
为实现双方安全通信提供了电子认证。
在因特网、公司内部网或外部网中，使用数字证书实现身份识别和电子信息加密。
数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证。

83、SSL 证书
SSL 证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。
因为配置在服务器上，也称为 SSL 服务器证书。

84、防火墙
主要部署于不同网络或网络安全域之间的出口，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，有选择地接受外部访问。

85、IDS
入侵检测系统，用于在黑客发起进攻或是发起进攻之前检测到攻击，并加以拦截。

IDS 是不同于防火墙。防火墙只能屏蔽入侵，而 IDS 却可以在入侵发生以前，通过一些信息来检测到即将发生的攻击或是入侵并作出反应。

86、NIDS
是 Network Intrusion Detection System 的缩写，即网络入侵检测系统，主要用于检测 Hacker 或 Cracker 。
通过网络进行的入侵行为。NIDS 的运行方式有两种，一种是在目标主机上运行以监测其本身的通信信息，另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，比如 Hub、路由器。

87、IPS
全称为 Intrusion-Prevention System，即入侵防御系统，目的在于及时识别攻击程序或有害代码及其克隆和变种，采取预防措施，先期阻止入侵，防患于未然。
或者至少使其危害性充分降低。入侵预防系统一般作为防火墙 和防病毒软件的补充来投入使用。

88、杀毒软件
也称反病毒软件或防毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件等计算机威胁的一类软件。

89、反病毒引擎
通俗理解，就是一套判断特定程序行为是否为病毒程序（包括可疑的）的技术机制。

90、防毒墙
区别于部署在主机上的杀毒软件，防毒墙的部署方式与防火墙类似，主要部署于网络出口，用于对病毒进行扫描和拦截，因此防毒墙也被称为反病毒网关。

91、老三样
通常指 IDS、防火墙和反病毒三样历史最悠久安全产品。

92、告警
指网络安全设备对攻击行为产生的警报。

93、误报
也称为无效告警，通常指告警错误，即把合法行为判断成非法行为而产生了告警。
目前，由于攻击技术的快速进步和检测技术的限制，误报的数量非常大，使得安全人员不得不花费大量时间来处理此类告警，已经成为困扰并拉低日常安全处置效率的主要原因。
94、
漏报
通常指网络安全设备没有检测出非法行为而没有产生告警。一旦出现漏报，将大幅增加系统被入侵的风险。

95、NAC
全称为 Network Access Control，即网络准入控制，其宗旨是防止病毒和蠕虫等新兴黑客

技术对企业安全造成危害。
借助 NAC，客户可以只允许合法的、值得信任的终端设备（例如 PC、服务器、PDA）接入网络，而不允许其它设备接入。

96、漏扫
即漏洞扫描，指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

97、UTM
即 Unified Threat Management，中文名为统一威胁管理，最早由 IDC 于 2014 年提出，即将不同设备的安全能力（最早包括入侵检测、防火墙和反病毒技术），集中在同一网关上，实现统一管理和运维。

98、网闸
网闸是使用带有多种控制功能的固态开关读写介质，连接两个独立主机系统的信息安全设备。
由于两个独立的主机系统通过网闸进行隔离，只有以数据文件形式进行的无协议摆渡。

99、堡垒机
运用各种技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为，以便集中报警、及时处理及审计定责。

100、数据库审计
能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。
它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

101、DLP
数据防泄漏，通过数字资产的精准识别和策略制定，主要用于防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业。

102、VPN
虚拟专用网，在公用网络上建立专用网络，进行加密通讯，通过对数据包的加密和数据包目标地址的转换实现远程访问。

103、SD-WAN
即软件定义广域网，这种服务用于连接广阔地理范围的企业网络、数据中心、互联网应用及

104、云服务。
这种服务的典型特征是将网络控制能力通过软件方式云化。
通常情况下，SD-WAN 都集成有防火墙、入侵检测或者防病毒能力。并且从目前的趋势来看，以安全为核心设计的 SD-WAN 正在崭露头角，包括 Fortinet 等多家安全厂商开始涉足该领域，并提供了较为完备的内生安全设计。

105、路由器
是用来连接不同子网的中枢，它们工作于 OSI7 层模型的传输层和网络层。
路由器的基本功能就是将网络信息包传输到它们的目的地。一些路由器还有访问控制列表（ACLs），允许将不想要的信息包过滤出去。
许多路由器都可以将它们的日志信息注入到 IDS 系统中，并且自带基础的包过滤（即防火墙）功能。

106、网关
通常指路由器、防火墙、IDS、VPN 等边界网络设备。

107、WAF
即 Web Application Firewall，即 Web 应用防火墙，是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。

108、SOC
即 Security Operations Center，翻译为安全运行中心或者安全管理平台，通过建立一套实时的资产风险模型，协助管理员进行事件分析、风险分析、预警管理和应急响应处理的集中安全管理系统。

109、LAS
日志审计系统，主要功能是提供日志的收集、检索和分析能力，可为威胁检测提供丰富的上下文。

110、NOC
即 Network Operations Center，网络操作中心或网络运行中心，是远程网络通讯的管理、监视和维护中心，是网络问题解决、软件分发和修改、路由、域名管理、性能监视的焦点。

111、SIEM
即 Security Information and Event Management，安全信息和事件管理，负责从大量企业安全控件、主机操作系统、企业应用和企业使用的其他软件收集安全日志数据，并进行分析和报告。

112、上网行为管理
是指帮助互联网用户控制和管理对互联网使用的设备。
其包括对网页访问过滤、上网隐私保护、网络应用控制、带宽流量管理、信息收发审计、用户行为分析等。

113、蜜罐（Honeypot）
是一个包含漏洞的系统，它摸拟一个或多个易受攻击的主机，给黑客提供一个容易攻击的目标。
由于蜜罐没有其它任务需要完成，因此所有连接的尝试都应被视为是可疑的。
蜜罐的另一个用途是拖延攻击者对其真正目标的攻击，让攻击者在蜜罐上浪费时间。
蜜罐类产品包括蜜网、蜜系统、蜜账号等等。

114、沙箱
沙箱是一种用于安全的运行程序的机制。它常常用来执行那些非可信的程序。
非可信程序中的恶意代码对系统的影响将会被限制在沙箱内而不会影响到系统的其它部分。

115、沙箱逃逸
一种识别沙箱环境，并利用静默、欺骗等技术，绕过沙箱检测的现象

116、网络靶场
主要是指通过虚拟环境与真实设备相结合，模拟仿真出真实赛博网络空间攻防作战环境，能够支撑攻防演练、安全教育、网络空间作战能力研究和网络武器装备验证试验平台。

2. 技术与服务

117、加密技术
加密技术包括两个元素：算法和密钥。

算法是将普通的文本与一串数字（密钥）的结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解码的一种算法。

密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。相应地，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

118、黑名单
顾名思义，黑名单即不好的名单，凡是在黑名单上的软件、IP 地址等，都被认为是非法的。

119、白名单
与黑名单对应，白名单即“好人”的名单，凡是在白名单上的软件、IP 等，都被认为是合法的，可以在计算机上运行。

120、内网
通俗的讲就是局域网，比如网吧、校园网、公司内部网等都属于此类。
查看 IP 地址，如果是在以下三个范围之内，就说明我们是处于内网之中的：10.0.0.0—10.255.255.255，172.16.0.0—172.31.255.255，192.168.0.0—192.168.255.255

121、外网
直接连入 INTERNET（互连网），可以与互连网上的任意一台电脑互相访问。

122、边界防御
以网络边界为核心的防御模型，以静态规则匹配为基础，强调把所有的安全威胁都挡在外网。

123、南北向流量
通常指数据中心内外部通信所产生的的流量。

124、东西向流量
通常指数据中心内部不同主机之间互相通信所产生的的流量。

125、规则库
网络安全的核心数据库，类似于黑白名单，用于存储大量安全规则，一旦访问行为和规则库完成匹配，则被认为是非法行为。所以有人也将规则库比喻为网络空间的法律。

126、下一代
网络安全领域经常用到，用于表示产品或者技术有较大幅度的创新，在能力上相对于传统方法有明显的进步，通常缩写为 NG（Next Gen）。
例如 NGFW（下一代防火墙）、NGSOC（下一代安全管理平台）等。

127、大数据安全分析
区别于传统被动规则匹配的防御模式，以主动收集和分析大数据的方法，找出其中可能存在的安全威胁，因此也称数据驱动安全。

128、EPP
全称为 Endpoint Protection Platform，翻译为端点保护平台，部署在终端设备上的安全防护解决方案,用于防止针对终端的恶意软件、恶意脚本等安全威胁,通常与 EDR 进行联动。

129、EDR
全称 Endpoint Detection & Response，即端点检测与响应，通过对端点进行持续检测，同时通过应用程序对操作系统调用等异常行为分析，检测和防护未知威胁，最终达到杀毒软件无法解决未知威胁的目的。

130、NDR
全称 Network Detection & Response，即网络检测与响应，通过对网络侧流量的持续检测和分析，帮助企业增强威胁响应能力，提高网络安全的可见性和威胁免疫力。

131、安全可视化
指在网络安全领域中的呈现技术，将网络安全加固、检测、防御、响应等过程中的数据和结果转换成图形界面，并通过人机交互的方式进行搜索、加工、汇总等操作的理论、方法和技术。

132、NTA
网络流量分析（NTA）的概念是 Gartner 于 2013 年首次提出的，位列五种检测高级威胁的手段之一。
它融合了传统的基于规则的检测技术，以及机器学习和其他高级分析技术，用以检测企业网络中的可疑行为，尤其是失陷后的痕迹。

133、MDR

全称 Managed Detection & Response，即托管检测与响应，依靠基于网络和主机的检测工具来识别恶意模式。
此外，这些工具通常还会从防火墙之内的终端收集数据，以便更全面地监控网络活动。

134、应急响应
通常是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。

135、XDR
通常指以检测和响应技术为核心的网络安全策略的统称，包括 EDR、NDR、MDR 等。

136、安全运营
贯穿产品研发、业务运行、漏洞修复、防护与检测、应急响应等一系列环节，实行系统的管理方法和流程，将各个环节的安全防控作用有机结合，保障整个业务的安全性。
137、威胁情报
根据 Gartner 的定义，威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。根据使用对象的不同，威胁情报主要分为人读情报和机读情报。

138、TTP
主要包括三要素，战术 Tactics、技术 Techniques 和过程 Procedures，是描述高级威胁组织及其攻击的重要指标，作为威胁情报的一种重要组成部分，TTP 可为安全分析人员提供决策支撑。

139、IOC
中文名为失陷标示：用以发现内部被 APT 团伙、木马后门、僵尸网络控制的失陷主机，类型上往往是域名、URL 等。
目前而言，IOC 是应用最为广泛的威胁情报，因为其效果最为直接。一经匹配，则意味着存在已经失陷的主机。

140、上下文
从文章的上下文引申而来，主要是指某项威胁指标的关联信息，用于实现更加精准的安全匹配和检测。

141、STIX
STIX 是一种描述网络威胁信息的结构化语言，能够以标准化和结构化的方式获取更广泛的网络威胁信息，常用于威胁情报的共享与交换，目前在全球范围内使用最为广泛。
STIX 在定义了 8 中构件的 1.0 版本基础上，已经推出了定义了 12 中构件的 2.0 版本。

142、杀伤链
杀伤链最早来源于军事领域，用于描述进攻一方各个阶段的状态。
在网络安全领域，这一概念最早由洛克希德-马丁公司提出，英文名称为 Kill Chain，也称作网络攻击生命周期，包括侦查追踪、武器构建、载荷投递、漏洞利用、安装植入、命令控

制、目标达成等七个阶段，来识别和防止入侵。

143、ATT&CK
可以简单理解为描述攻击者技战术的知识库。
MITRE 在 2013 年推出了该模型，它是根据真实的观察数据来描述和分类对抗行为。
ATT&CK 将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式（STIX）、指标信息的可信自动化交换（TAXII）来表示。

144、钻石模型
钻石模型在各个领域的应用都十分广泛，在网络安全领域，钻石模型首次建立了一种将科学原理应用于入侵分析的正式方法：
可衡量、可测试和可重复——提供了一个对攻击活动进行记录、(信息)合成、关联的简单、正式和全面的方法。
这种科学的方法和简单性可以改善分析的效率、效能和准确性。

145、关联分析
又称关联挖掘，就是在交易数据、关系数据或其他信息载体中，查找存在于项目集合或对象集合之间的频繁模式、关联、相关性或因果结构。
在网络安全领域主要是指将不同维度、类型的安全数据进行关联挖掘，找出其中潜在的入侵行为。

146、态势感知
是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

147、探针
也叫作网络安全探针或者安全探针，可以简单理解为赛博世界的摄像头，部署在网络拓扑的关键节点上，用于收集和分析流量和日志，发现异常行为，并对可能到来的攻击发出预警。

148、网络空间测绘
用搜索引擎技术来提供交互，让人们可以方便的搜索到网络空间上的设备。
相对于现实中使用的地图,用各种测绘方法描述和标注地理位置,用主动或被动探测的方法，来绘制网络空间上设备的网络节点和网络连接关系图，及各设备的画像。

149、SOAR
全称 Security Orchestration, Automation and Response，意即安全编排自动化与响应，主要通过剧本化、流程化的指令，对入侵行为采取的一系列自动化或者半自动化响应处置动作。

150、UEBA
全称为 User and Entity Behavior Analytics，即用户实体行为分析，一般通过大数据分析的方法，分析用户以及 IT 实体的行为，从而判断是否存在非法行为。

151、内存保护
内存保护是操作系统对电脑上的内存进行访问权限管理的一个机制。内存保护的主要目的是防止某个进程去访问不是操作系统配置给它的寻址空间。

152、RASP
全称为 Runtime application self-protection，翻译成应用运行时自我保护。
在 2014 年时由 Gartner 提出，它是一种新型应用安全保护技术，它将保护程序像疫苗一样注入到应用程序中，应用程序融为一体，能实时检测和阻断安全攻击，使应用程序具备自我保护能力，当应用程序遭受到实际攻击伤害，就可以自动对其进行防御，而不需要进行人工干预。

153、包检测
对于流量包、数据包进行拆包、检测的行为。

155、深度包检测
Deep Packet Inspection,缩写为 DPI,又称完全数据包探测(complete packet inspection)或信息萃取（Information eXtraction，IX），是一种计算机网络数据包过滤技术，用来检查通过检测点之数据包的数据部分(亦可能包含其标头)，以搜索不匹配规范之协议、病毒、垃圾邮件、入侵迹象。

156、全流量检测
全流量主要体现在三个“全”上，即全流量采集与保存，全行为分析以及全流量回溯。
通过全流量分析设备，实现网络全流量采集与保存、全行为分析与全流量回溯，并提取网络元数据上传到大数据分析平台实现更加丰富的功能。

157、元数据
元数据（Metadata），又称中介数据、中继数据，为描述数据的数据（data about data），主要是描述数据属性(property)的信息，用来支持如指示存储位置、历史数据、资源查找、文件记录等功能。

158、欺骗检测
以构造虚假目标来欺骗并诱捕攻击者,从而达到延误攻击节奏,检测和分析攻击行为的目的。

159、微隔离
顾名思义是细粒度更小的网络隔离技术，能够应对传统环境、虚拟化环境、混合云环境、容器环境下对于东西向流量隔离的需求,重点用于阻止攻击者进入企业数据中心网络内部后的横向平移。

160、逆向
常见于逆向工程或者逆向分析，简单而言，一切从产品中提取原理及设计信息并应用于再造及改进的行为，都是逆向工程。
在网络安全中，更多的是调查取证、恶意软件分析等。

161、无代理安全
在终端安全或者虚拟化安全防护中，往往需要在每一台主机或者虚机上安装 agent（代理程序）来实现，这种方式往往需要消耗大量的资源。
而无代理安全则不用安装 agent，可以减少大量的部署运维工作，提升管理效率。

162、CWPP
全称 Cloud Workload Protection Platform，意为云工作负载保护平台，主要是指对云上应用和工作负载（包括虚拟主机和容器主机上的工作负载）进行保护的技术，实现了比过去更加细粒度的防护，是现阶段云上安全的最后一道防线。

163、CSPM
云安全配置管理，能够对基础设施安全配置进行分析与管理。这些安全配置包括账号特权、网络和存储配置、以及安全配置（如加密设置）。如果发现配置不合规，CSPM 会采取行动进行修正。
164、CASB
全称 Cloud Access Security Broker，即云端接入安全代理。作为部署在客户和云服务商之间的安全策略控制点，是在访问基于云的资源时企业实施的安全策略。

165、防爬
意为防爬虫，主要是指防止网络爬虫从自身网站中爬取信息。网络爬虫是一种按照一定的规则，自动地抓取网络信息的程序或者脚本。

166、安全资源池
安全资源池是多种安全产品虚拟化的集合，涵盖了服务器终端、网络、业务、数据等多种安全能力。

167、IAM
全称为 Identity and Access Management，即身份与访问管理，经常也被叫做身份认证。

168、4A
即认证 Authentication、授权 Authorization、账号 Account、审计 Audit，即融合统一用户账号管理、统一认证管理、统一授权管理和统一安全审计四要素后的解决方案将，涵盖单点登录（SSO）等安全功能。

169、Access Control list(ACL)
访问控制列表。

170、多因子认证
主要区别于单一口令认证的方式，要通过两种以上的认证机制之后，才能得到授权，使用计算机资源。
例如，用户要输入 PIN 码，插入银行卡，最后再经指纹比对，通过这三种认证方式，才能获得授权。这种认证方式可以降低单一口令失窃的风险，提高安全性。

171、特权账户管理

简称 PAM。由于特权账户往往拥有很高的权限，因此一旦失窃或被滥用，会给机构带来非常大的网络安全风险。所以，特权账户管理往往在显得十分重要。
其主要原则有：杜绝特权凭证共享、为特权使用赋以个人责任、为日常管理实现最小权限访问模型、对这些凭证执行的活动实现审计功能。

172、零信任
零信任并不是不信任，而是作为一种新的身份认证和访问授权理念，不再以网络边界来划定可信或者不可信，而是默认不相信任何人、网络以及设备，采取动态认证和授权的方式，把访问者所带来的的网络安全风险降到最低。

173、SDP
全称为 Software Defined Perimeter，即软件定义边界，由云安全联盟基于零信任网络提出，是围绕某个应用或某一组应用创建的基于身份和上下文的逻辑访问边界。

174、Security as a Service
安全即服务，通常可理解为以 SaaS 的方式，将安全能力交付给客户。

175、同态加密
同态加密是一类具有特殊自然属性的加密方法，此概念是 Rivest 等人在 20 世纪 70 年代首先提出的，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能。

177、量子计算
是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式，目前已经逐渐应用于加密和通信传输。

177、可信计算
是一项由可信计算组（可信计算集群，前称为 TCPA）推动和开发的技术。
可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。

178、拟态防御
核心实现是一种基于网络空间内生安全机理的动态异构冗余构造（Dynamic Heterogeneous Redundancy，DHR），为应对网络空间中基于未知漏洞、后门或病毒木马等的未知威胁，提供具有普适创新意义的防御理论和方法。

179、区块链
英文名为 blockchain，它是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”、“全程留痕”、“可以追溯”、“公开透明”、“集体维护”等特征。

180、远程浏览器
鉴于浏览器往往成为黑客攻击的入口，因此将浏览器部署在远程的一个“浏览器服务器池”中。
这样一来，这些浏览器所在的服务器跟用户所在环境中的终端和网络是隔离的，从而使得客

户所在网络的暴露面大大降低。
这种服务也类似于虚拟桌面、云手机等产品。

181、云手机
云手机采用全新的 VMI（Virtual Mobile Infrastructure 虚拟移动设施，与 PC 云桌面类似）技术，为员工提供一个独立的移动设备安全虚拟手机，业务应用和数据仅在服务端运行和存储，个人终端上仅做加密流媒体呈现和触控，从而有效保障企业数据的安全性。

182、风控
也称大数据风控，是指利用大数据分析的方法判断业务可能存在的安全风险，目前该技术主要用于金融信贷领域，防止坏账的发生。

183、渗透测试
为了证明网络防御按照预期计划正常运行而提供的一种机制，通常会邀请专业公司的攻击团队，按照一定的规则攻击既定目标，从而找出其中存在的漏洞或者其他安全隐患，并出具测试报告和整改建议。
其目的在于不断提升系统的安全性。

184、安全众测
借助众多白帽子的力量，针对目标系统在规定时间内进行漏洞悬赏测试。
您在收到有效的漏洞后，按漏洞风险等级给予白帽子一定的奖励。通常情况下是按漏洞付费，性价比较高。
同时，不同白帽子的技能研究方向可能不同，在进行测试的时候更为全面。

185、内生安全
指的是不断从信息化系统内生长出的安全能力，能伴随业务的增长而持续提升，持续保证业务安全。
内生安全有三个特性，即依靠信息化系统与安全系统的聚合、业务数据与安全数据的聚合以及 IT 人才和安全人才的聚合，从信息化系统的内部，不断长出自适应、自主和自成长的安全能力。

188、内生安全框架
该框架从顶层视角出发，支撑各行业的建设模式从“局部整改外挂式”，走向“深度融合体系化”；从工程实现的角度，将安全需求分步实施，逐步建成面向未来的安全体系；内生安全框架能够输出实战化、体系化、常态化的安全能力，构建出动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的网络安全防御体系。

内生安全框架包含了总结出了 29 个安全区域场景和 89 类安全组件。

188、PPDR
英文全称为 Policy Protection Detection Response，翻译为策略、防护、检测和响应。
主要以安全策略为核心，通过一致性检查、流量统计、异常分析、模式匹配以及基于应用、目标、主机、网络的入侵检查等方法进行安全漏洞检测。

188、CARTA
全称为 Continuous Adaptive Risk and Trust Assessment，即持续自适应风险与信任评估旨在通过动态智能分析来评估用户行为，放弃追求完美的安全，不能要求零风险，不要求 100%信任，寻求一种 0 和 1 之间的风险与信任的平衡。
CARTA 战略是一个庞大的体系，其包括大数据、AI、机器学习、自动化、行为分析、威胁检测、安全防护、安全评估等方面。

189、SASE
全称为 Secure Access Service Edge，即安全访问服务边缘，Gartner 将其定义为一种基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。
实体的身份可与人员、人员组（分支办公室）、设备、应用、服务、物联网系统或边缘计算场地相关联。

190、SDL
全称为 Security Development Lifecycle，翻译为安全开发生命周期，是一个帮助开发人员构建更安全的软件和解决安全合规要求的同时降低开发成本的软件开发过程，最早由微软提出。

191、DevSecOps
全称为 Development Security Operations，可翻译为安全开发与运维。
它强调在 DevOps 计划刚启动时就要邀请安全团队来确保信息的安全性，制定自动安全防护计划，并贯穿始终，实现持续 IT 防护。

192、代码审计
顾名思义就是检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

193、NTLM 验证
NTLM(NT LAN Manager)是微软公司开发的一种身份验证机制，从 NT4 开始就一直使用，主要用于本地的帐号管理。

194、MTTD
平均检测时间。

195、MTTR
平均响应时间。

197、CVE
全称 Common Vulnerabilities and Exposures，由于安全机构 Mitre 维护一个国际通用的漏洞唯一编号方案，已经被安全业界广泛接受的标准。

197、软件加壳

“壳”是一段专门负责保护软件不被非法修改或反编译的程序。
它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。
经过加壳的软件在跟踪时已无法看到其真实的十六进制代码，因此可以起到保护软件的目的。

198、CNVD
国家信息安全漏洞共享平台，由国家计算机应急响应中心 CNCERT 维护，主要负责统一收集、管理国内的漏洞信息，其发布的漏洞编号前缀也为 CNVD。

199、数据脱敏
数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护，主要用于数据的共享和交易等涉及大范围数据流动的场景。

200、GDPR
《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）为欧洲联盟的条例，前身是欧盟在 1995 年制定的《计算机数据保护法》。

201、CCPA
美国加利福尼亚州消费者隐私保护法案。

202、SRC
即 Security Response Center，中文名为安全应急响应中心，主要职责为挖掘并公开收集机构存在的漏洞和其他安全隐患。

203、CISO
有时也被叫做 CSO，即首席信息安全官，为机构的主要安全负责人。

204、IPC 管道
为了更好地控制和处理不同进程之间的通信和数据交换，系统会通过一个特殊的连接管道来调度整个进程。

205、SYN 包
TCP 连接的第一个包，非常小的一种数据包。SYN 攻击包括大量此类的包，由于这些包看上去来自实际不存在的站点，因此无法有效进行处理。

206、IPC$
是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

207、shell
指的是一种命令指行环境，是系统与用户的交换方式界面。简单来说，就是系统与用户“沟通”的环境。
我们平时常用到的 DOS，就是一个 shell。（Windows2000 是 cmd.exe）

208、ARP
地址解析协议(Address Resolution Protocol)此协议将网络地址映射到硬件地址。

安全圈，有很多「技术黑话」

外行人听了一脸懵逼

内行人看了笑而不语

大家深知

多少生意，都藏在这些黑话里

这些“黑话”很简单、很熟悉

资深的安全圈从业者都能如数家珍

因为大家每天，都在与之打交道

为威胁生，为漏洞死，为攻防辛苦一辈子

吃 DDoS 亏，上 APT 当，最后挂在 0 day 上

感谢这些黑话，给我们带来万亿生意

敬畏这些黑话，让我们时刻保持警惕