第一部分：关键词

[渗透入门篇] 渗透行业必备术语大集合(一)

肉鸡、抓鸡、堡垒机、木马、大马

小马、挂马、网页木马、一句话木马、后门

一句话后门、Shell、webshell、交互 shell、远控

托库、社工库、撞库、社会工程学、权限

提权、弱口令、溢出、Root、rootkit

[渗透入门篇] 渗透行业必备术语大集合(二)

IPC$、默认共享 、注入、注入点、C 段渗透

旁段入侵、内网、外网、脚本注入攻击、中间人攻击

欺骗攻击、ARP 攻击、CC 攻击、拒绝服务攻击、Dos 攻击

DDos、洪水攻击、SYN 攻击、供应链攻击、鱼叉攻击

钓鲸攻击、水坑攻击、APT 攻击、商业电子邮件攻击、电信诈骗

[渗透入门篇] 渗透行业必备术语大集合(三)

网络钓鱼、社会工程学攻击、假托、蜜罐、免杀

花指令、加壳、脱壳、软件加壳、软件脱壳

渗透测试、渗透、黑盒测试、白盒测试、灰盒测试

黑帽黑客、白帽黑客、红帽黑客、红队、蓝队

紫队、ip 地址、端口、端口扫描、反弹端口

[渗透入门篇] 渗透行业必备术语大集合(四)

端口映射、路由器、交换机、网关、独立服务器

proxy、WAF、防火墙、反病毒引擎、防毒墙

IDS、NIDS、IPS、规则库、侵预

告警、漏报、NAC、上网行为管理、下一代

VPN、边界防御、蠕虫病毒、杀毒软件、恶意软件

[渗透入门篇] 渗透行业必备术语大集合(五)

间谍软件、反间谍软件、黑产、灰产、暗网

黑页、薅羊毛、杀猪盘、威胁情报、加密技术

对称加密、非对称加密、加密机、嗅探、探针

跳板、RARP、UDP、TCP、FTP

SNTP、SMTP、TELNET、HTTP、HTTPS

[渗透入门篇] 渗透行业必备术语大集合(六)

ICMP、DNS、CDN、TCP/IP、OSI

LAN、MAN、WAN、EXP、POC

payload、shellcode、HTML、CSS、Javascript

CMS、VPS、源损耗、域名、URL

cURL、URI、URN、CTF、AWD

[渗透入门篇] 渗透行业必备术语大集合(七)

CVE、SRC、CNVD、0day、1day

Nday、C2、横移、暴库、CA 证书

数字证书、SSL 证书、数字签名、漏扫、UTM

网闸、数据库审计、DLP、SD-WAN、SOC

SIEM、MIME、沙箱、沙箱逃逸、网络靶场

[渗透入门篇] 渗透行业必备术语大集合(八)

黑名单、白名单、南北向流量、东西向流量、大数据安全分析

杀伤链、网络空间测绘、逆向、防爬、安全资源池

区块链、安全众测、代码审计、数据脱敏、箱子

漏洞复现、软件木马、脚本木马、3899 肉鸡、4899 肉鸡

缓冲区溢出、嗅探器、CMD、powershell、常见端口

目录

6. 小马（小马）

7. 挂马（挂马）

8. 网页木马（网页木马）

9. 一句话木马（一句话木马）

10. 后门（后门）

11. 一句话后门（一句话后门）

12. Shell（shell）

13. webshell（webshelwebshell）

14. 交互式 shell（交互式 shell）

15. 远控（远控）

16. 拖库（拖库）

17. 社工库（社工库）

18. 撞库（撞库）

19. 社会工程学（社会工程学）

20. 权限（权限）

21. 提权（提权）

22. 弱口令（弱口令）

23. 溢出（溢出）

24. Root（root）

25. rootkit

[渗透入门篇] 渗透行业必备术语大集合(二)

1. IPC$（IPC$）

2. 默认共享 （默认共享）

3. 注入（注入）

4. 注入点（注入点）

5. C 段渗透

6. 旁站入侵（旁注）

7. 内网（局域网）

8. 外网（广域网）

9. 脚本注入攻击（sql 注入）

10. 中间人攻击（中间人攻击）

11. 欺骗攻击（欺骗攻击）

12. ARP 攻击（ARP 攻击）

13. CC 攻击（CC 攻击）

14. 拒绝服务攻击（拒绝服务攻击）

15. Dos 攻击（DOS 攻击）

16. DDOS（DDOS）

17. 洪水攻击（洪水攻击）

18. SYN 攻击（SYN 攻击）

19. 供应链攻击

20. 鱼叉攻击（鱼叉攻击）

21. 钓鲸攻击（钓鲸攻击）

22. 水坑攻击（水坑攻击）

23. APT 攻击（APT 攻击）

24. 商业电子邮件攻击（BEC）（电子邮件攻击）

25. 电信诈骗（电信诈骗）

[渗透入门篇] 渗透行业必备术语大集合(三)

1. 网络钓鱼（钓鱼攻击）

2. 社会工程学攻击（社会工程攻击）

3. 假托（假托）

4. 蜜罐（蜜罐）

5. 免杀（免杀）

6. 花指令（花指令）

7. 加壳（加壳）

8. 脱壳（脱壳）

9. 软件加壳（加壳）

10. 软件脱壳（软件脱壳）

11. 渗透测试（渗透测试）

12. 渗透（渗透）渗透测试类型

13. 黑盒测试（黑盒测试）渗透测试类型

14. 白盒测试（白盒测试）渗透测试类型

15. 灰盒测试（灰盒测试）渗透测试类型

16. 黑帽黑客（黑帽黑客）

17. 白帽黑客（白帽黑客）

18. 红帽黑客（红客）

19. 红队（红队）

20. 蓝队（蓝队）

21. 紫队（紫队）

22. ip 地址（ip 地址）

23. 端口（端口）

24. 端口扫描（端口扫描）

25. 反弹端口（反弹端口原理）

[渗透入门篇] 渗透行业必备术语大集合(四)

1. 端口映射（端口映射）

2. 路由器（路由器）

3. 交换机（交换机）

4. 网关（网关）

5. 独立服务器（独立服务器）

6. proxy（proxy）

7. WAF（WAF）

8. 防火墙（防火墙）

9. 反病毒引擎（杀毒引擎）

10. 防毒墙（防毒墙）

11. IDS（入侵检测系统）

12. NIDS（网络入侵检测系统）

13. IPS（入侵防御系统）

14. 规则库（规则库）

15. 侵预（侵预）

16. 告警（告警）

17. 漏报（漏报）

18. NAC（NAC）

19. 上网行为管理（上网行为管理）

20. 下一代（下一代防火墙）

21. VPN（虚拟专用网络）

22. 边界防御（边界防御）

23. 蠕虫病毒（蠕虫病毒）

24. 杀毒软件（杀毒软件）

25. 恶意软件（流氓软件）

[渗透入门篇] 渗透行业必备术语大集合(五)

1. 间谍软件（间谍软件）

2. 反间谍软件（反间谍软件）

3. 黑产（网络黑产）

4. 灰产（灰产）

5. 暗网（暗网）

6. 黑页（黑页）

7. 薅羊毛（薅羊毛）

8. 杀猪盘（杀猪盘）

9. 威胁情报（威胁情报）

10. 加密技术（加密技术）

11. 对称加密（对称加密）

12. 非对称加密（非对称加密）

13. 加密机（加密机）

14. 嗅探（嗅探）

15. 探针（探针）

16. 跳板（跳板）

17. RARP（RARP）

18. UDP（UDP）

19. TCP（TCP）

20. FTP（FTP）

21. SNTP（SNTP）

22. SMTP（SMTP）

23. TELNET（TELNET）

24. HTTP（HTTP）

25. HTTPS（HTTPS）

[渗透入门篇] 渗透行业必备术语大集合(六)

1. ICMP（ICMP）

2. DNS（DNS）

3. CDN（CDN）

4. TCP/IP（TCP/IP）

5. OSI（OSI）

6. LAN（LAN）

7. MAN（MAN）

8. WAN（WAN）

9. EXP（EXPloit）

10. POC（Proof of Concept）

11. payload（payload）

12. shellcode（shellcode）

13. HTML（HTML）

14. CSS（CSS）

15. Javascript（Javascript）

16. CMS（内容管理系统）

17. VPS（VPS）

18. 源损耗（损耗）

19. 域名（域名）

20. url（统一资源定位符）

21. URI（统一资源标识符）

22. URN（统一资源名称）

23. curl（curl）

24. CTF（CTF）

25. AWD（AWD）

[渗透入门篇] 渗透行业必备术语大集合(七)

1. CVE（CVE）

2. SRC（SRC）

3. CNVD（国家信息安全漏洞共享平台）

4. 0day（0day）

5. 1day（1day）

6. Nday（Nday）

7. C2（C2）

8. 横移（横移）

9. 暴库（暴库）

10. CA 证书（CA 证书）

11. 数字证书（数字证书）

12. SSL 证书（SSL 证书）

13. 数字签名（数字签名）

14. 漏扫（漏洞扫描）

15. UTM（UTM）

16. 网闸（网闸）

17. 数据库审计（数据库审计）

第二部分：关键词解释

[渗透入门篇] 渗透行业必备术语大集合(一)

肉鸡、抓鸡、堡垒机、木马、大马

小马、挂马、网页木马、一句话木马、后门

一句话后门、Shell、webshell、交互 shell、远控

托库、社工库、撞库、社会工程学、权限

提权、弱口令、溢出、Root、rootkit

---

1. 肉鸡（肉鸡）

肉鸡也称傀儡机，是指可以被黑客远程控制的机器。比如用"灰鸽子"等诱导客户点击或者电脑被黑客攻破或用户电脑有漏洞被种植了木马，黑客可以随意操纵它并利用它做任何事情。

简单来说：肉鸡是一种很形象的比喻，比喻那些可以随意被我们控制的电脑，可以是各种系统。可以是普通的个人电脑，也可以是大型的服务器，我们可以象操作自己的电脑那样来操作它们，而不被对方所发觉。

肉鸡通常被用作 DDOS 攻击。可以是各种系统，如 windows、linux、unix 等，更可以是一家公司、企业、学校甚至是政府军队的服务器。

2. 抓鸡（抓鸡）

抓鸡是黑客界的一种流行语言.这里所说的"鸡",是指电脑肉鸡、网络摄像头、路由器、等联网设备。

简单来说：就是想尽一切办法控制电脑，将其沦为肉鸡。

3. 堡垒机（堡垒机）

简单来说：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。

堡垒机综合了核心系统运维和安全审计管控两大主干功能。终端计算机对目标的访问，均需要经过运维安全审计的翻译。

4. 木马（木马）

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击 Dos 等特殊功能的后门程序。

木马病毒其实是计算机黑客用于远程控制计算机的程序，将控制程序寄生于被控制的计算机系统中，里应外合，对被感染木马病毒的计算机实施操作。

一般的木马病毒程序主要是寻找计算机后门，伺机窃取被控计算机中的密码和重要文件等。

可以对被控计算机实施监控、资料修改等非法操作。木马病毒具有很强的隐蔽性，可以根据黑客意图突然发起攻击。

简单来说：木马就是那些表面上伪装成了正常的程序，但是当这些被程序运行时，就会获取系统的整个控制权限，是具备破坏和删除文件、发送密码、记录键盘和攻击 Dos 等特殊功能的后门程序。

有很多黑客就是热中与使用木马程序来控制别人的电脑，比如灰鸽子，黑洞，PcShare 等等

5. 大马（大马）

特点：体积大，功能全，会调用系统的关键函数，以代码加密进行隐藏的 webshell

简单来说：功能强大的网页后门，能执行命令，操作文件，连接数据库

6. 小马（小马）

特点：体积小，功能少，只有一个上传功能的 webshell。

简单来说：比较单一的网页后门。一般是上传保存大马。asp 小马 asp 旁注小马

7. 挂马（挂马）

所谓的挂马，就是黑客通过各种手段，包括 SQL 注入，网站敏感文件扫描，服务器漏洞，网站程序 0day,等各种方法获得网站管理员账号，然后登陆网站后台，通过数据库“备份/恢复”或者上传漏洞获得一个 webshell。

利用获得的 webshell 修改网站页面的内容，向页面中加入恶意转向代码。

也可以直接通过弱口令获得服务器或者网站 FTP，然后直接对网站页面直接进行修改。

当你访问被加入恶意代码的页面时，你就会自动的访问被转向的地址或者下载木马病毒。

简单来说：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

8. 网页木马（网页木马）

简单来说：表面上伪装成普通的网页文件或是将自己的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下载到访问者的电脑上来自动执行。

网页木马并不是木马程序，而应该称为网页木马“种植器”，也即一种通过攻击浏览器或浏览器外挂程序的漏洞，向目标用户机器植入木马、病毒、密码盗取等恶意程序的手段

9. 一句话木马（一句话木马）

简单来说：短小精悍的木马，而且功能强大，隐蔽性非常好，在入侵中始终扮演着强大的作用。

10. 后门（后门）

后门，本意是指一座建筑背面开设的门，通常比较隐蔽，为进出建筑的人提供方便和隐蔽。在信息安全领域，后门是指绕过安全控制而获取对程序或系统访问权的方法。后门的最主要目的就是方便以后再次秘密进入或者控制系统。

简单来说：这是一种形象的比喻，攻击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。

这些改动表面上是很难被察觉的，但是攻击者却可以使用相应的程序或者方法来轻易的与这台电脑建立连接，重新控制这台电脑，就好象是攻击者偷偷的配了一把主人房间的要是，可以随时进出而不被主人发现一样。

通常大多数的特洛伊木马（TrojanHorse）程序都可以被攻击者用语制作后门（BackDoor）

11. 一句话后门（一句话后门）

一句话后门是 Web 渗透中用得最多的一个必备工具，流行一句话后门分为 Asp、Asp.net、Jsp 和 Php 四种类型。

一句话后门利用的实质就是通过执行 SQL 语句、添加或者更改字段内容等操作。

简单来说：一段很小的网页代码后门，可以用客户端连接，对网站进行控制。如中国菜刀。服务端是一句话后门。

12. Shell（shell）

在计算机科学中，Shell 俗称壳（用来区别于核），是指为使用者提供操作界面的软件。它类似于 DOS 下的 COMMAND.COM 和后来的 CMD.exe。它接收用户命令，然后调用相应的应用程序。

简单来说：就是指的是一种命令指行环境，比如我们按下键盘上的“开始键+R”时出现“运行”对话框，在里面输入“cmd”会出现一个用于执行命令的黑窗口，这个就是 WINDOWS 的 Shell 执行环境。

通常我们使用远程溢出程序成功溢出远程电脑后得到的那个用于执行系统命令的环境就是对方的 shell

13. webshell（webshelwebshell）

简单来说就是：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。

webshell 分类：根据脚本可以分为 PHP 脚本木马，ASP 脚本木马，也有基于.NET 的脚本木马和 JSP 脚本木马。根绝时代和技术的变迁，国外也有用 python 编写的脚本木马，不过国内常用的无外乎三种，大马，小马，一句话木马，具体使用场景和特地如下图。

国内常用的 webshell 有海阳 ASP 木马，Phpspy，c99shell 等

黑客在入侵了一个网站后，通常会将 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

可以上传下载文件，查看数据库，执行任意程序命令等。

14. 交互式 shell（交互式 shell）

简单来说：交互式模式就是 shell 等待你的输入，并且执行你提交的命令。

这种模式被称作交互式是因为 shell 与用户进行交互。

这种模式也是大多数用户非常熟悉的：登录、执行一些命令、签退。当你签退后，shell 也终止了。

shell 也可以运行在另外一种模式：非交互式模式。在这种模式下，shell 不与用户进行交互，而是读取存放在文件中的命令，并且执行它们。当它读到文件的结尾，shell 也就终止了。

15. 远控（远控）

简单来说：就是远程控制，是在网络上由一台电脑（主控端 Remote/客户端）远距离去控制另一台电脑（被控端 Host/服务器端）的技术。

这里的远程不是字面意思的远距离，一般指通过网络控制远端电脑。

16. 拖库（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。到了黑客攻击泛滥的今天，它被用来指网站遭到入侵后，黑客窃取其数据库文件，拖库的主要防护手段是数据库加密。

拖库可以通过数据库安全防护技术解决，数据库安全技术主要包括：数据库加密，防火墙，数据脱敏等。

简单来说：黑客入侵数据库后把数据库导出来。

17. 社工库（社工库）

社工库是黑客与大数据方式进行结合的一种产物，黑客们将泄漏的用户数据整合分析，然后集中归档的一个地方

这些用户数据大部分来自社工库论坛上，黑客们脱库撞库获得的数据包，包含的数据类型除了账号密码外，还包含被攻击网站所属不同行业所带来的附加数据。

简单来说：社工库是黑客的一种攻击方式，去获取敏感信息。

18. 撞库（撞库）

简单来说：撞库是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。

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，这就可以理解为撞库攻击。

撞库可采用大数据安全技术来防护，比如：用数据资产梳理发现敏感数据，使用数据库加密保护核心数据，使用数据库安全运维防运维人员撞库攻击等。

19. 社会工程学（社会工程学）

社会工程学（Social Engineering，又被翻译为：社交工程学）在上世纪60年代左右作为正式的学科出现。

广义社会工程学的定义是：建立理论并通过利用自然的、社会的和制度上的途径来逐步地解决各种复杂的社会问题，经过多年的应用发展，社会工程学逐渐产生出了分支学科，如公安社会工程学和网络社会工程学。

简单来说：社会工程学攻击是一种通过对被攻击者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱所采取的诸如欺骗、伤害等危害手段，获取自身利益的手法。

20. 权限（权限）

权限是指为了保证职责的有效履行，任职者必须具备的，对某事项进行决策的范围和程度。

在多用户计算机系统的管理中，权限（privilege）是指某个特定的用户具有特定的系统资源使用权力，像是文件夹，特定系统指令的使用或存储量的限制。

通常，系统管理员，或者在网络中的网络管理员，对某个特定资源的使用分配给用户不同的权限，系统软件则自动地强制执行这些权限。

简单来说：权限计算机用户对于文件及目录的建立，修改，删除以及对于某些服务的访问，程序的执行，是以权限的形式来严格区分的。被赋予了相应的权限，就可以进行相应的操作，否则就不可以。

21. 提权（提权）

提权，顾名思义就是提高自己在服务器中的权限，就比如在windows中你本身登录的用户是
guest，然后通过提权后就变成超级管理员，拥有了管理Windows的所有权限。

提权是黑客的专业名词，一般用于网站入侵和系统入侵中。

22. 弱口令（弱口令）

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。

弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，因此不推荐用户使用。

简单来说：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）、常见 top100、top1000 弱口令

23. 溢出（溢出）

溢出是黑客利用操作系统的漏洞，专门开发了一种程序，加相应的参数运行后，就可以得到你电脑具有管理员资格的控制权，你在你自己电脑上能够运行的东西他可以全部做到，等于你的电脑就是他的了。溢出是程序设计者设计时的不足所带来的错误。

溢出：确切的讲，应该是“缓冲区溢出”。简单的解释就是程序对接受的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。大致可以分为两类：1. 堆溢出　2. 栈溢出

24. Root（root）

Root，也称为根用户，是 Unix 和类 UNIX 系统，及 Android 和 iOS 移动设备系统中的唯一的超级用户，因其可对根目录执行读写和执行操作而得名。其相当于 windows 系统中的 system(XP 及以下)/trustedlnstaller(Vista 及以上)用户。其具有系统中的最高权限，如启动或停止一个进程，删除或增加用户，增加或者禁用硬件，新建文件、修改文件或删除所有文件等等。

简单来说：这里的 root 指在 Linux 里面 root 是代表最高权限

25. rootkit

Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是 Rootkit 一般都和木马、后门等其他恶意程序结合使用。

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，对方系统内存在的安全漏洞获得系统的 root 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 与我们前边提到的木马和后门很类似，但远比它们要隐蔽，黑客守卫者就是很典型的 rootkit，还有国内的 ntroorkit 等都是不错的 rootkit 工具。

[渗透入门篇] 渗透行业必备术语大集合(二)

IPC$、默认共享 、注入、注入点、C 段渗透

旁段入侵、内网、外网、脚本注入攻击、中间人攻击

欺骗攻击、ARP 攻击、CC 攻击、拒绝服务攻击、Dos 攻击

DDos、洪水攻击、SYN 攻击、供应链攻击、鱼叉攻击

钓鲸攻击、水坑攻击、APT 攻击、商业电子邮件攻击、电信诈骗

---

1. IPC$（IPC$）

空连接，使用命令 net use *.*.*.*（IP 地址）\ipc$ "" /user:"" 就可以简单地和目标建立一个空连接（需要目标开放 ipc$）。

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饿命名管道，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。

利用 IPC$,连接者可以与目标主机建立一个空的连接，即无需用户名和密码就能连接主机，当然这样连接是没有任何操作权限的。但利用这个空的连接，连接者可以得到目标主机上的用户列表。

网上关于 ipc$ 入侵的文章可谓多如牛毛，攻击步骤甚至已经成了固化的模式，因此也没人愿意再把这已经成为定式的东西拿出来摆弄。

要防止别人用 ipc$和默认共享入侵，需要禁止 ips$空连接，避免入侵者取得用户列表，并取消默认共享。

2. 默认共享 （默认共享）

默认共享：默认共享是 WINDOWS2000/XP/2003 系统开启共享服务时自动开启所有硬盘的共享，因为加了"$"符号，所以看不到共享的托手图表，也成为隐藏共享，和上面写的 IPC$ 一样。

在 Windows 2000/XP/2003 系统中，逻辑分区与 Windows 目录默认为共享，这是为管理员管理服务器的方便而设，但却成为了别有用心之徒可乘的安全漏洞。

3. 注入（注入）

注入：随着 B/S 模式应用开发的发展，使用这种模式编写程序的程序员越来越来越多，但是由于程序员的水平参差不齐相当大一部分应用程序存在安全隐患。

用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想要知道的数据，这个就是所谓的 SQLinjection，即：SQL 恶意注入。

SQL 注入即是指 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，从而进一步得到相应的数据信息。

4. 注入点（注入点）

注入点：是可以实行注入的地方，通常是一个访问数据库的连接。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

举个例子来说：注入点好比化作一条大街，小偷顺着大街走，发现有一家侧门没有关，进去后找到可以拿的东西卖出去，注入点就是侧门。

很多网站被黑无非是找到注入点拿到网站后台然后找出管理员账号密码来进行登录，登陆成功后百分之八十都会用到一句话木马.得到网站的 webshell，得到了服务器提权后远控。

5. C 段渗透

C 段下服务器入侵同一个网段内例如 202.202.0.1-2020.0.254 如果拿下其中一台服务器，通过这台服务器嗅探目标服务器传输上的数据，从而获取这台服务器的权限。

常见的工具有 cain。

简单来说：就是对同局域网内的其他主机进行渗透，以此来获取目标主机权限。

6. 旁站入侵（旁注）

旁注是一种入侵方法，在字面上解释就是"从旁注入"，利用同一主机上面不同网站的漏洞得到 webshell，从而利用主机上的程序或者是服务所暴露的用户所在的物理路径进行入侵。

简单来说：就是同一个服务器上有多个站点，可以通过入侵其中一个站点，通过提权跨目录访问其他站点

7. 内网（局域网）

局域网自然就是局部地区形成的一个区域网络，其特点就是分布地区范围有限，可大可小，大到一栋建筑楼 与相邻建筑之间的连接，小到可以是办公室之间的联系。

局域网自身相对其他网络传输速度更快，性能更稳定，框架简易，并且是封闭性，这也是很多机构选择的原因所在。

简单来讲：就是局域网，比如网吧，公司网络，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的话，就说明我们是处于内网之中的：（私网 IP　）

10.0.0.0—10.255.255.255，172.16.0.0—172.31.255.255，192.168.0.0—192.168.255.255

8. 外网（广域网）

广域网，又称外网、公网。是连接不同地区局域网或城域网计算机通信的远程网。通

常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个地区、城市和国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。

广域网并不等同于互联网。

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，IP 地址不是保留 IP（内网）IP 地址。

9. 脚本注入攻击（sql 注入）

所谓脚本注入攻击者把 SQL 命令插入到 WEB 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令，在某些表单中，用户输入的内容直接用来构造动态的 SQL 命令，或作为存储过程的输入参数，这类表单特别容易受到 SQL 注入式攻击

10. 中间人攻击（中间人攻击）

中间人攻击（Man-in-the-MiddleAttack，简称“MITM 攻击”）中间人攻击很早就成为了黑客常用的一种古老的攻击手段，并且一直到如今还具有极大的扩展空间。

在网络安全方面，MITM 攻击的使用是很广泛的，曾经猖獗一时的 SMB 会话劫持、DNS 欺骗等技术都是典型的 MITM 攻击手段。

在黑客技术越来越多的运用于以获取经济利益为目标的情况下时，MITM 攻击成为对网银、网游、网上交易等最有威胁并且最具破坏性的一种攻击方式。

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，这台计算机就称为“中间人”。

11. 欺骗攻击（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

12. ARP 攻击（ARP 攻击）

ARP（AddressResolutionProtocol，地址解析协议）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。

一般情况下，受到 ARP 攻击的计算机会出现两种现象：

1. 不断弹出“本机的 XXX 段硬件地址与网络中的 XXX 段地址冲突”的对话框。
2. 计算机不能正常上网，出现网络中断的症状。

因为这种攻击是利用 ARP 请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截。因此普通的防火墙很难抵挡这种攻击。

ARP 病毒攻击是局域网最常见的一种攻击方式。

由于 TCP/IP 协议栈存在的一些漏洞给 ARP 病毒有进行欺骗攻击的机会，ARP 利用 TCP/IP 协议的漏洞进行欺骗攻击，现已严重影响到人们正常上网和通讯安全。

当局域网内的计算机遭到 ARP 的攻击时，它就会持续地向局域网内所有的计算机及网络通信设备发送大量的 ARP 欺骗数据包，如果不及时处理，便会造成网络通道阻塞、网络设备的承载过重、网络的通讯质量不佳等情况。

13. CC 攻击（CC 攻击）

攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装就叫：CC(ChallengeCollapsar)

CC 主要是用来攻击页面的。大家都有这样的经历，就是在访问论坛时，如果这个论坛比较大，访问的人比较多，打开页面的速度会比较慢，访问的人越多，论坛的页面越多，数据库压力就越大，被访问的频率也越高，占用的系统资源也就相当可观。

原理：攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。

简单来说：就是在一些大的网站不断地发送大量的搜索请求，消耗服务器资源。

14. 拒绝服务攻击（拒绝服务攻击）

拒绝服务攻击 （DOS）造成 DOS 的攻击行为被称为 DOS 攻击，其目的是使计算机或网络无法正常服务，最常见的 DOS 攻击有计算机网络宽带攻击和连通性攻击，连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源被消耗，最终计算机无法再处理合法用户的请求。

实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。

拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为网络协议本身的安全缺陷，从而拒绝服务攻击也成为了攻击者的终极手法。

攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：

一是迫使服务器的缓冲区满，不接收新的请求；

二是使用 IP 欺骗，迫使服务器把非法用户的连接复位，影响合法用户的连接 。

简单来说：就是攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。

15. Dos 攻击（DOS 攻击）

DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络宽带攻击和连通性攻击。

拒绝服务攻击。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

DoS 攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。

这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。

这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。

16. DDOS（DDOS）

分布式拒绝服务攻击可以使很多的计算机在同一时间遭受到攻击，使攻击的目标无法正常使用，分布式拒绝服务攻击已经出现了很多次，导致很多的大型网站都出现了无法进行操作的情况，这样不仅仅会影响用户的正常使用，同时造成的经济损失也是非常巨大的。

分布式拒绝服务攻击方式在进行攻击的时候，可以对源 IP 地址进行伪造，这样就使得这种攻击在发生的时候隐蔽性是非常好的，同时要对攻击进行检测也是非常困难的，因此这种攻击方式也成为了非常难以防范的攻击。

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。

17. 洪水攻击（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。

常见的还有洪水攻击包含：MAC 泛洪、网络泛洪等。

常见的洪水攻击方式：阿拉丁洪水攻击器、ARP 攻击、DDOS 攻击。

18. SYN 攻击（SYN 攻击）

SYN 攻击是黑客攻击的手段。

SYN 洪泛攻击的基础是依靠 TCP 建立连接时三次握手的设计。

第三个数据包验证连接发起人在第一次请求中使用的源 IP 地址上具有接受数据包的能力，即其返回是可达的。

据统计，在所有黑客攻击事件中，SYN 攻击是最常见又最容易被利用的一种攻击手法。

如：2000 年 YAHOO 网站遭受的攻击事例

有些网络蠕虫病毒配合 SYN 攻击造成更大的破坏。

19. 供应链攻击

供应链攻击是一种面向软件开发人员和供应商的新兴威胁。

目标是通过感染合法应用分发恶意软件来访问源代码、构建过程或更新机制。

简单来说：就是是黑客攻击目标机构的合作伙伴，并以该合作伙伴为跳板，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！

原理：攻击者寻找不安全的网络协议、未受保护的服务器基础结构和不安全的编码做法。 它们将在生成和更新过程中中断、更改源代码以及隐藏恶意软件。

由于软件由受信任的供应商构建和发布，因此这些应用和更新已签名并经过认证。

在软件供应链攻击中，供应商可能未意识到他们的应用或更新在发布到公众时受到恶意代码的感染。 然后，恶意代码将以与应用相同的信任和权限运行。

20. 鱼叉攻击（鱼叉攻击）

鱼叉攻击是计算机病毒术语，通常是指利用木马程序作为电子邮件的附件，发送到目标电脑上，诱导受害者去打开附件来感染木马。

鱼叉攻击是将用鱼叉捕鱼形象的引入到了网络攻击中，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"。

如：

2014 年 05 月 22 新疆发生了致死 31 人的暴力恐怖性事件之后，5 月 28 日，该黑客组织曾发送名为“新疆暴恐事件最新通报”的电子邮件及附件，引诱目标人群“中招”。

该组织曾发送过的电邮名称还包括“公务员工资收入改革方案”等一系列社会高度关注的热点，令人防不胜防。

21. 钓鲸攻击（钓鲸攻击）

所谓 "鲸钓攻击" （Whaling Attack）指的就是针对高层管理人员的欺诈和商业电子邮件骗局。

BEC 诈骗又称钓鲸欺诈，攻击者要么侵入公司电子邮件账户，要么冒充承包商或商务合作伙伴，发送网络钓鱼邮件提交虚假发票。

只要发票被支付，资金便会汇入银行，然后被快速洗走。

简单来说：钓鲸攻击是另一种进化形式的鱼叉式网络钓鱼，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。

22. 水坑攻击（水坑攻击）

"水坑攻击"，黑客攻击方式之一，顾名思义，是在受害者必经之路设置了一个"水坑(陷阱)"。

最常见的做法是，黑客分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，先将此网站"攻破"并植入攻击代码，一旦攻击目标访问该网站就会"中招"。

水坑攻击属于 APT 攻击的一种，与鱼叉攻击相比，黑客无需耗费精力制作钓鱼网站，而是利用合法网站的弱点，隐蔽性比较强。

水坑攻击主要针对的目标多为特定的团体（组织、行业、地区等）。

攻击者首先通过猜测（或观察）确定这组目标经常访问的网站，并入侵其中一个或多个，植入恶意软件，最后，达到感染该组目标中部分成员的目的。

由于此种攻击借助了目标团体所信任的网站，攻击成功率很高，即便是那些对鱼叉攻击或其他形式的钓鱼攻击具有防护能力的团体。

23. APT 攻击（APT 攻击）

APT 攻击（AdvancedPersistentThreat 攻击）：即高级可持续威胁攻击,也称为定向威胁攻击，指某组织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。

特点：极强的隐蔽性、潜伏期长，持续性强、目标性强

24. 商业电子邮件攻击（BEC）（电子邮件攻击）

电子邮件攻击，是商业应用最多的一种商业攻击，我们也将它称为邮件炸弹攻击，就是对某个或多个邮件发送大量的邮件，使网络流量加大占用处理器时间，消耗系统资源，从而使系统瘫痪。

有许多邮件炸弹软件，虽然它们的操作有所不同，成功率也不稳定，但是有一点就是他们可以隐藏攻击者不被发现。

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

25. 电信诈骗（电信诈骗）

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。如：

冒充公检法、商家公司厂家、国家机关工作人员、银行工作人员等各类机构工作人员，伪造和冒充招工、刷单、贷款、手机定位和招嫖等形式进行诈骗。

从 2000 年新千年以来，随着科技的发展，一系列技术工具的开发出现和被使用，许多技术人员和一些平民借助于手机、固定电话、网络等通信工具和现代的技术等实施的非接触式的诈骗可以说是迅速地发展蔓延，给人民群众造成了很大的损失。

电信诈骗

网络钓鱼、社会工程学攻击、假托、蜜罐、免杀

花指令、加壳、脱壳、软件加壳、软件脱壳

渗透测试、渗透、黑盒测试、白盒测试、灰盒测试

黑帽黑客、白帽黑客、红帽黑客、红队、蓝队

紫队、ip 地址、端口、端口扫描、反弹端口

---

1. 网络钓鱼（钓鱼攻击）

网络钓鱼（Phishing，与钓鱼的英语 fishing 发音相近，又名钓鱼法或钓鱼式攻击）是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID 、 ATM PIN 码或信用卡详细信息）的一种攻击方式。

网络钓鱼 （Phishing）攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。

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。

如今的"网络钓鱼"攻击利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、口令和社保编号等内容

2. 社会工程学攻击（社会工程攻击）

社会工程攻击，是一种利用"社会工程学" 来实施的网络攻击行为。

社会工程学攻击是一种通过对被攻击者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱所采取的诸如欺骗、伤害等危害手段，获取自身利益的手法。

所有社会工程学攻击都建立在使人决断产生认知偏差的基础上。有时候这些偏差被称为“人类硬件漏洞”，足以产生众多攻击方式。如：假托、调虎离山、在线聊天、等价交换等等。

黑客社会工程学攻击则是将黑客入侵攻击手段进行了最大化，不仅能够利用系统的弱点进行入侵，还能通过人性的弱点进行入侵，当黑客攻击与社会工程学攻击融为一体时，将根本不存在所谓安全的系统

3. 假托（假托）

假托（pretexting）是一种社交工程（social engineering）的形式，其中个体通过欺诈来获取特权数据。假托是一种虚假的动机。

假托（pretexting）是一种制造虚假情形，以迫使针对受害人吐露平时不愿泄露的信息的手段。该方法通常预含对特殊情景专用术语的研究，以建立合情合理的假象。

假托（pretexting）通常是一个骗局，欺骗者在骗局中假装需要信息来确认对话人的身份。

在和目标对象建立信任之后，假托者可能会问一系列问题来收集关键的个人身份信息，如确认个人社会保险号、母亲的婚前姓、出生地或日期或者是帐户号。

4. 蜜罐（蜜罐）

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机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

简单来说：好比是情报收集系统。故意让人攻击的目标，引诱黑客来攻击，所以攻击者攻击后，你就可以知道他是如何得逞的，随时了解针对你的服务器发动的最新的攻击和漏洞。

还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络，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。

5. 免杀（免杀）

免杀技术全称为反杀毒技术 *Anti Anti- Virus* 简称"免杀"，它指的是一种能使病毒木马免于被杀毒软件查杀的技术。

由于免杀技术的涉猎面非常广，其中包含反汇编、逆向工程、系统漏洞等黑客技术，所以难度很高，一般人不会或没能力接触这技术的深层内容。其内容基本上都是修改病毒、木马的内容改变特征码，从而躲避了杀毒软件的查杀。

简单来说：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。

6. 花指令（花指令）

花指令是，由设计者特别构思，希望使反汇编的时候出错，让破解者无法清楚正确地反汇编内容的内容，迷失方向。

经典的是，目标位置是另一条指令的中间，这样在反汇编的时候便会出现混乱。

花指令有可能利用各种指令：jmp，call，ret 的一些技巧堆栈，位置运算，等等。

简单来说：就是几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常的判断病毒文件的构造。

再通俗点就是杀毒软件是从头到脚按顺序来查找病毒。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。

7. 加壳（加壳）

加壳的全称应该是可执行程序资源压缩，压缩后的程序可以直接运行。

加壳的另一种常用的方式是在二进制的程序中植入一段代码，在运行的时候优先取得程序的控制权，之后再把控制权交还给原始代码，这样做的目的是隐藏程序真正的 OEP（入口点，防止被破解）。大多数病毒就是基于此原理。

加壳的程序需要阻止外部程序或软件对加壳程序本身的反汇编分析或者动态分析，以达到保护壳内原始程序以及软件不被外部程序破坏，保证原始程序正常运行。

这种技术也常用来保护软件版权，防止软件被破解。但对于病毒，加壳可以绕过一些杀毒软件的扫描，从而实现它作为病毒的一些入侵或破坏的一些特性。

简单来说：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。

8. 脱壳（脱壳）

在一些计算机软件里有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。

由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”。

软件加壳是作者写完软件后，为了保护自己的代码或维护软件产权等利益所常用到的手段。有很多加壳工具，既然有盾，自然就有矛，脱壳即去掉软件所加的壳，软件有手动脱和自动脱壳之分，

9. 软件加壳（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。

10. 软件脱壳（软件脱壳）

软件脱壳，顾名思义，就是对软件加壳的逆操作，把软件上存在的壳去掉。

在一些计算机软件里也有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。

由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”了。

就像计算机病毒和自然界的病毒一样，其实都是命名上的方法罢了。

11. 渗透测试（渗透测试）

简单来说：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全安全的一种评估方法。

这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

渗透测试，是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。

不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了漏洞扫描器等工具，以确保所有补丁都已打上。

如果你早已做到了这些，为什么还要请外方进行审查或渗透测试呢？

因为，渗透测试能够独立地检查你的网络策略，换句话说，就是给你的系统安了一双眼睛。

而且，进行这类测试的，都是寻找网络系统安全漏洞的专业人士。

渗透测试包括：黑盒测试、白盒测试、灰盒测试

12. 渗透（渗透）渗透测试类型

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。

黑客技术里的渗透是指黑客通过非法途径入侵网站系统，拿到网站的 WebShell 进行非法操作。也指信息安全风险评估。

13. 黑盒测试（黑盒测试）渗透测试类型

渗透黑盒测试与软件黑盒测试有一点区别。

软件黑盒测试：

它是通过测试来检测每个功能是否都能正常使用。

在测试中，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息。

黑盒测试着眼于程序外部结构，不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。渗透测试类型

黑盒测试是以用户的角度，从数据输入与输出数据的对应关系出发进行测试的。

渗透黑盒测试：

经过授权的黑盒测试是设计成为模拟攻击者的入侵行为，并在不了解客户组织大部分信息和知识的情况下实施的。黑盒测试可以用来测试内部安全团队检测和应对一次攻击的能力。

黑盒测试比较费时，同时对技术要求比较高。

在安全业界的渗透测试眼中，黑盒测试能更逼真地模拟了一次真正的攻击过程。

黑盒测试依靠测试人员的能力探测获取目标系统的信息，作为一次黑盒测试的渗透测试者，通常不需要找出目标系统的所有安全漏洞，而只需要尝试找出并利用可以获取目标系统访问权代价最小的攻击路径，并保证不被检测到。

渗透届黑盒测试一般指不知道源码，无法进行代码审计的测试。

14. 白盒测试（白盒测试）渗透测试类型

渗透百合测试与软件白盒测试有一点区别。

软件白盒测试：

白盒测试又称结构测试、透明盒测试、逻辑驱动测试或基于代码的测试。

白盒测试是一种测试用例设计方法，盒子指的是被测试的软件，白盒指的是盒子是可视的，即清楚盒子内部的东西以及里面是如何运作的。

"白盒"法全面了解程序内部逻辑结构、对所有逻辑路径进行测试。

"白盒"法是穷举路径测试。在使用这一方案时，测试者必须检查程序的内部结构，从检查程序的逻辑着手，得出测试数据。贯穿程序的独立路径数是天文数字。

渗透白盒测试：

使用白盒测试，需要和客户组织一起工作，来识别出潜在的安全风险。

白盒测试的最大好处是测试者将拥有所有的内部知识，并可以在不需要害怕被阻断的情况下任意地实施破坏。

而白盒测试最大的问题在于无法有效地测试客户组织的应急响应程序，也无法判断出他们的安全防护计划对检测特定攻击的效率。

白盒测试适用于时间比较紧急，或是特定的渗透测试环境如情报收集并不在范围之内的测试场景。

渗透届黑盒测试一般指知道源码，可以进行代码审计的测试。

15. 灰盒测试（灰盒测试）渗透测试类型

软件灰盒测试：

灰盒测试，是介于白盒测试与黑盒测试之间的一种测试，灰盒测试多用于集成测试阶段，不仅关注输出、输入的正确性，同时也关注程序内部的情况。

灰盒测试不像白盒那样详细、完整，但又比黑盒测试更关注程序的内部逻辑，常常是通过一些表征性的现象、事件、标志来判断内部的运行状态。

渗透灰盒测试：

以上两种渗透测试基本类型的组合可以提供对目标系统更加深入和全面的安全审查，这就是灰盒测试（Grey-box Testing），组合之后的好处就是能够同时发挥两种基本类型渗透测试方法的各自优势。

灰盒测试需要渗透测试者能够根据对目标系统所掌握的有限知识与信息，来选择评估整体安全性的最佳途径。

在采用灰盒测试方法的外部渗透场景中，渗透测试者也类似地需要从外部逐步渗透进入目标网络，但他所拥有的目标网络底层拓扑与架构将有助于更好地决策攻击途径与方法，从而达到更好的渗透测试效果。

16. 黑帽黑客（黑帽黑客）

与白帽黑客相反，黑帽黑客(black hat hacker)就是人们常说的“黑客”或“骇客”了。

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。

他们往往利用自身技术，在网络上窃取别人的资源或破解收费的软件，以达到获利。

虽然在他们看来这是因为技术而就得到的，但是这种行为却往往破坏了整个市场的秩序，或者泄露了别人的隐私。

简单来说：为了非法目进行黑客攻击的人。

17. 白帽黑客（白帽黑客）

白帽黑客网络用语中指站在黑客的立场攻击自己的系统以进行安全漏洞排查的程序员。

他们用的是黑客惯用的破坏攻击的方法，行的却是维护安全之事。

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。

18. 红帽黑客（红客）

红客(Honker(A person or thing that honks))是指维护国家利益，不利用网络技术入侵自己国家电脑，而是"维护正义，为自己国家争光的黑客"。

红客是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神并热爱着计算机技术的都可称为红客。

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。**

简单来说：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。

19. 红队（红队）

通常指攻防演习中的攻击队伍

20. 蓝队（蓝队）

通常指攻防演习中的防守队伍

21. 紫队（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

22. ip 地址（ip 地址）

internet 上的电脑有许多，为了让他们能够相互识别，internet 上的每一台主机都分配有一个唯一的 32 位地址，该地址称为 ip 地址，也称作网际地址，ip 地址由 4 个数值部分组成，每个数值部分可取值 0-255，各部分之间用一个‘.‘分开

IP 地址（Internet Protocol Address）是指互联网协议地址，又译为网际协议地址。

IP 地址是 IP 协议提供的一种统一的地址格式，它为互联网上的每一个网络和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。

23. 端口（端口）

端口：（Port）相当于一种数据的传输通道。

用于接受某些数据，然后传输给相应的服务，而电脑将这些数据处理后，再将相应的恢复通过开启的端口传给对方。

一般每一个端口的开放的偶对应了相应的服务，要关闭这些端口只需要将对应的服务关闭就可以了

24. 端口扫描（端口扫描）

端口扫描是指某些别有用心的人发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型（这些网络服务均与端口号相关）。

端口扫描是计算机解密高手喜欢的一种方式。

攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。

扫描器是一种自动检测远程或本机主机安全性弱点的程序，通过使用扫描器你可以不留痕迹的发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本！

这就能让我们间接的或直观的了解到远程主机所存在的安全问题。

简单来说：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。

25. 反弹端口（反弹端口原理）

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。

简单地说，就是由木马的服务端主动连接客户端所在 IP 对应的电脑的 80 端口。相信没有哪个防火墙会拦截这样的连接（因为它们一般认为这是用户在浏览网页），所以反弹端口型木马可以穿墙。

[渗透入门篇] 渗透行业必备术语大集合(四)

端口映射、路由器、交换机、网关、独立服务器

proxy、WAF、防火墙、反病毒引擎、防毒墙

IDS、NIDS、IPS、规则库、侵预

告警、漏报、NAC、上网行为管理、下一代

VPN、边界防御、蠕虫病毒、杀毒软件、恶意软件

---

1. 端口映射（端口映射）

端口映射是 NAT 的一种，功能是把在公网的地址转翻译成私有地址， 采用路由方式的 ADSL 宽带路由器拥有一个动态或固定的公网 IP，ADSL 直接接在 HUB 或交换机上，所有的电脑共享上网。

端口映射功能可以让内部网络中某台机器对外部提供 WWW 服务，这不是将真 IP 地址直接转到内部提供 www 服务的主机。

2. 路由器（路由器）

路由器（Router）是连接两个或多个网络的硬件设备，在网络间起网关的作用，是读取每一个数据包中的地址然后决定如何传送的专用智能性的网络设备。

它能够理解不同的协议，例如某个局域网使用的以太网协议，因特网使用的 TCP/IP 协议。

这样，路由器可以分析各种不同类型网络传来的数据包的目的地址，把非 TCP/IP 网络的地址转换成 TCP/IP 地址，或者反之；再根据选定的路由算法把各数据包按最佳路线传送到指定位置。

所以路由器可以把非 TCP/IP 网络连接到因特网上。

简单来说：路由器的主要作用就是路由选择，将 IP 数据包正确的送到目的地，因此也叫 IP 路由器，外网装换为内网的东西，由 dns 转换。路由器是在网络上使用最高的设备之一。

3. 交换机（交换机）

交换机（Switch）意为"开关"是一种用于电（光）信号转发的网络设备。

它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。

4. 网关（网关）

网关(Gateway)又称网间连接器、协议转换器。

网关在网络层以上实现网络，是复杂的网络互连设备，仅用于两个高层协议不同的网络互连。网关既可以用于广域网互连，也可以用于局域网互连。

网关是一种充当转换重任的计算机系统或设备。使用在不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关是一个翻译器。

与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。同层---应用层。

通常指路由器、防火墙、IDS、VPN 等边界网络设备。

5. 独立服务器（独立服务器）

独立服务器一般指独立 IP 主机。独立 IP 主机是指在服务器上用一定的技术划分出多个空间以后，在每个虚拟主机上配上独立的 ip。

独立服务器整体硬件都是独立的，性能强大，特别是 CPU，被认为是性能最佳的托管选项之一。

使用真实存在的独立服务器就像拥有自己的房子，没有人打扰，可以部署任何想要的东西。

简单来说：就是整台服务器只有一个用户享有，只有一人使用。拥有独立的 IP、内存、带宽、硬盘，可以使用任何系统，可以运行各种网站及配置各种网站环境，对访问量也没有限制。

6. proxy（proxy）

指的是代理软件或代理服务器，也可以认为是一种网络访问方式。

代理类，用来进行事物不想或不能进行的其他操作，比如当你对数据库进行操作时，代理可以在你对数据库操作完后，记录下你所进行的操作。

简单来说：代理，一类程序或系统，接收来自客户机算计的流量，并代表客户与服务器交互。

代理能用于过滤应用级别的制定类型的流量或缓存信息以提高性能。许多防火墙依赖代理进行过滤

7. WAF（WAF）

Web 应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall，简称： WAF）。

国际上公认的一种说法：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。

简单来说：就是为应用层提供防护的防火墙。

8. 防火墙（防火墙）

防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术。

防火墙技术的功能主要在于及时发现并处理计算机网络运行时可能存在的安全风险、数据传输等问题，其中处理措施包括隔离与保护，同时可对计算机网络安全当中的各项操作实施记录与检测，以确保计算机网络运行的安全性，保障用户资料与信息的完整性，为用户提供更好、更安全的计算机网络使用体验。

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。

9. 反病毒引擎（杀毒引擎）

反病毒引擎其实就是杀毒引擎，又叫做 AV。

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。

杀毒引擎是杀毒软件的主要部分。是去检测和发现病毒的程序。而病毒库是已经发现的病毒的标本。用病毒库中的标本去对照机器中的所有程序或文件，看是不是符合这些标本，是则是病毒，否就不一定是病毒（因为还有很多没有被发现的或者刚刚产生的病毒）。

10. 防毒墙（防毒墙）

人类步入了二十一世纪，信息产业飞速发展，互联网正在迅速地发展和普及。

伴随而来的是计算机病毒的日益猖狂。尽管许多企业已经具有了一定的安全防范意识，并且部署了网络版杀毒软件和硬件防火墙，但是在面对诸如 SQLSlammer 等新的蠕虫病毒时，仍然显得力不从心。

面对现今恶劣的互联网安全状况，只有强有力的防毒墙才能保障企业网络的安全。

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。

11. IDS（入侵检测系统）

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。

简单来说：就是起检测作用的，常常与 IPS 一起使用。

12. NIDS（网络入侵检测系统）

NIDS 是 NetworkIntrusion 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。

13. IPS（入侵防御系统）

入侵防御系统(IPS: Intrusion Prevention System)是电脑网络安全设施，是对防病毒软件（Antivirus Programs）和防火墙(Packet Filter, Application Gateway)的补充。

入侵防御系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够及时的终端、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。

简单来说：就是防御用的，IDS 是检测用的，常常一起使用。

14. 规则库（规则库）

规则库（rule base）是 2018 年公布的计算机科学技术名词。由规则组成的知识库。是基于规则的专家系统的重要组成部分。

简单来说：规则库就是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。

15. 侵预（侵预）

一般作为防火墙和防病毒软件的补充来投入使用。

16. 告警（告警）

系统发生故障时，监控单元将视故障情况给出告警信号，所有故障均有声光告警及文字提示。告警时，监控单元上的红色告警灯亮，蜂鸣声发出报警声，并向远端监控中心发出告警信息。

指网络安全设备对攻击行为产生的警报，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。

17. 漏报（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。

可以联想一下疫情，如果产生漏报产生危害的风险是很大的。

18. NAC（NAC）

全称为 NetworkAccess 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。

网络准入控制（NAC）是一项由思科发起、多家厂商参加的计划，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。

19. 上网行为管理（上网行为管理）

上网行为管理产品及技术是专用于防止非法信息恶意传播，避免国家机密、商业信息、科研成果泄漏的产品；并可实时监控、管理网络资源使用情况，提高整体工作效率。上网行为管理产品系列适用于需实施内容审计与行为监控、行为管理的网络环境，尤其是按等级进行计算机信息系统安全保护的相关单位或部门。

简单来说：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。

20. 下一代（下一代防火墙）

下一代，即 Next Generation。

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（NextGen）
例如：NGFW（下一代防火墙）、NGSOC（下一代安全管理平台）等

简单来说：就是创新较大的产品或者技术。

21. VPN（虚拟专用网络）

虚拟专用网络(VPN)的功能是：在公用网络上建立专用网络，进行加密通讯。

在企业网络中有广泛应用。VPN 网关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。

VPN 可通过服务器、硬件、软件等多种方式实现。

22. 边界防御（边界防御）

"边界防御"是国内知名安全企业金山率先提出的防病毒技术理念，该技术在金山毒霸 2012 中第一次应用。

与传统的防病毒技术理念最大的不同在于，"边界防御"强调"不中毒才是最佳安全解决方案"，通过对外界程序进入电脑的监控，在病毒尚未被运行时即可被判定为安全或不安全，从而最大限度地保障对本地计算机的安全防护。

23. 蠕虫病毒（蠕虫病毒）

蠕虫病毒是一种常见的计算机病毒，是无须计算机使用者干预即可运行的独立程序，它通过不停的获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据和恶意篡改系统。影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

它利用了 WINDOWS 系统的开放性特点，特别是 COM 到 COM+的组件编程思路，一个脚本程序能调用功能更大的组件来完成自己的功能。

以 VB 脚本病毒为例，它们都是把 VBS 脚本文件加在附件中，使用*.HTM，VBS 等欺骗性的文件名。

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

24. 杀毒软件（杀毒软件）

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。

杀毒软件通常集成监控识别、病毒扫描和清除、自动升级、主动防御等功能，有的杀毒软件还带有-数据恢复、防范黑客入侵、网络流量控制等功能，是计算机防御系统（包含杀毒软件，防火墙，特洛伊木马和恶意软件的查杀程序，入侵防御系统等）的重要组成部分。

杀毒软件是一种可以对病毒、木马等一切已知的对计算机有危害的程序代码进行清除的程序工具。“杀毒软件”由国内的老一辈反病毒软件厂商起的名字，后来由于和世界反病毒业接轨统称为"反病毒软件"、"安全防护软件"或"安全软件"。

集成防火墙的"互联网安全套装"、"全功能安全套装"等用于消除电脑病毒、特洛伊木马和恶意软件的一类软件，都属于杀毒软件范畴。

简单来说：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。

25. 恶意软件（流氓软件）

恶意软件其实就是"流氓软件"，是介于病毒和正规软件之间的软件。

如果电脑中有流氓软件，可能会出现以下几种情况：用户使用电脑上网时，会有窗口不断跳出；电脑浏览器被莫名修改增加了许多工作条；当用户打开网页时，网页会变成不相干的奇怪画面，甚至是黄色广告。

有些流氓软件只是为了达到某种目的，比如广告宣传。

这些流氓软件虽然不会影响用户计算机的正常使用，但在当用户启动浏览器的时候会多弹出来一个网页，以达到宣传目的。

简单来说：就是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。

[渗透入门篇] 渗透行业必备术语大集合(五)

间谍软件、反间谍软件、黑产、灰产、暗网

黑页、薅羊毛、杀猪盘、威胁情报、加密技术

对称加密、非对称加密、加密机、嗅探、探针

跳板、RARP、UDP、TCP、FTP

SNTP、SMTP、TELNET、HTTP、HTTPS

---

1. 间谍软件（间谍软件）

简单来说：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。

"间谍软件无处不在"，这是在计算机安全业界达成的共识。

据 IDC 在早前公布的数据中，估计大约 67%的电脑都带有某种形式的间谍软件，而在权威机构不久前进行的一次调查显示，在认为自己的个人电脑很“干净”的人中，经过检查 91%的接受调查者的计算机上都被安装了间谍软件。

2. 反间谍软件（反间谍软件）

"间谍软件无处不在"，这是在计算机安全业界达成的共识。

简单来说：反间谍软件就是发现和消灭间谍病毒的软件。

3. 黑产（网络黑产）

网络黑色产业链，是指利用互联网技术实施网络攻击、窃取信息、勒索诈骗、盗窃钱财、推广黄赌毒等网络违法行为，以及为这些行为提供工具、资源、平台等准备和非法获利变现的渠道与环节。

网络黑色产业链可分为上中下游：上游负责收集提供各种网络黑产资源，例如手机黑卡、动态代理等；中游负责开发定制大量黑产工具，以自动化手段组合利用各种黑产资源实施各种网络违法犯罪活动；下游负责将黑产活动“成果”进行交易变现，涉及众多黑灰色网络交易和支付渠道。

简单来说：网络黑产就是指以互联网为媒介，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

4. 灰产（灰产）

灰产，指处于法律灰色地带的"恶意注册"和"虚假认证"。

诈骗分子往往能够利用伪装的骗局以假乱真，达到骗取钱财的目的。

同时买卖公民个人信息、手机卡、银行卡、对公账户、工商营业执照、网络社交工具、网络支付账户等违法犯罪行为，为诈骗团伙提供犯罪工具，已成为助推电信网络诈骗犯罪的"黑灰产业"。

特点：

1. 骗局设计较为周密，模拟了互联网平台客户服务场景，从宣传引导到电话微信等客服交流，精心设计陷阱让首次接触的消费者难辨真假。

2. 借助移动支付手段，利用了互联网信息管理不完善的漏洞。

5. 暗网（暗网）

"暗网"是指隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权等才能登录。一般用 tor 洋葱浏览器进入。

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。

由于"暗网"具有匿名性等特点，容易滋生以网络为勾联工具的各类违法犯罪，一些年轻人深陷其中。

互联网是一个多层结构，"表层网"处于互联网的表层，能够通过标准搜索引擎进行访问浏览。藏在"表层网"之下的被称为"深网"。深网中的内容无法通过常规搜索引擎进行访问浏览。"暗网"通常被认为是"深网"的一个子集，显著特点是使用特殊加密技术刻意隐藏相关互联网信息。

2021 年 1 月，德国捣毁了据信是全球最大的暗网交易平台，逮捕了运行的嫌疑人。

6. 黑页（黑页）

一些计算机被入侵后，入侵者为了证明自己的存在，对网站主页（在服务器开放 WEB 服务的情况下）进行改写，从而公布入侵者留下的信息，这样的网页通常称为黑页。

黑页的意义：

黑页的意义有其消极的一方面，也有积极的一方面。

消极方面：

入侵者对网站主页的破坏，无疑会给网站带来经济、信誉等等方面的损失。

同时另一方面传播着入侵者留下的带有负面影响的信息或者病毒，严重影响网络安全。

积极方面：

对服务器管理人员作出最有效漏洞提醒，及时通知管理员打补丁。

同时也表现出入侵者的入侵目的。

7. 薅羊毛（薅羊毛）

薅羊毛，本是沿袭春晚小品中白云大妈的"薅羊毛织毛衣"的做法，被定义为"薅羊毛"。

所谓薅羊毛就是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。"薅羊毛"的定义已经不仅仅局限于互联网金融领域，已经渗透到社会各个领域，外卖优惠券、减免优惠、送话费、送流量等诸多活动，都可以称之为薅羊毛。

"薅羊毛"的定义越来越广泛，已经跨出了金融行业的界定，渗透到各个领域，嘀嘀打车等打车和拼车软件送代金券，美团外卖，饿了么点餐减免活动，百度钱包，免费送话费充流量等诸多活动，都可以称为薅羊毛。

简单来说：就是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的行为就被称之为薅羊毛。

8. 杀猪盘（杀猪盘）

杀猪盘是一个网络流行词，是指诈骗分子利用网络交友　，诱导受害人投资赌博的一种电信诈骗方式

。

"杀猪盘"是"从业者们"（诈骗团伙）自己起的名字，是指放长线"养猪"诈骗，养得越久，诈骗得越狠。

诈骗分子准备好人设、交友套路等"猪饲料"，将社交平台称为"猪圈"，在其中寻找被他们称为"猪"的诈骗对象。通过建立恋爱关系，即"养猪"。最后骗取钱财，即"杀猪"　。

各行各业都有托，卖酒的有酒托，卖茶的有茶托，卖摩托车的有车托，这些年网络赌博兴起，赌场也安排"赌托"到网上招揽生意，后来有人发现赌博什么的弱爆了，直接把人骗到假赌场一宰更省事，于是真假网赌混杂在一起，逐渐发展出一套全新的咋骗模式。

简单来说：杀猪盘就是以各种手段方式培养信任为基础，一段时间获得对方信任后，以各种诱惑让被害人受骗损失钱财为目的的诈骗方式。

9. 威胁情报（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。

业内大多数所说的威胁情报可以认为是狭义的威胁情报，其主要内容为用于识别和检测威胁的失陷标识，如文件 HASH，IP，域名，程序运行路径，注册表项等，以及相关的归属标签。

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。

威胁情报旨在为面临威胁的资产主体(通常为资产所属企业或机构)提供全面的、准确的、与其相关的、并且能够执行和决策的知识和信息。

10. 加密技术（加密技术）

加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）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密的一种算法。

在安全保密中，可通过适当的钥加密技术和管理机制来保证网络的信息通信安全

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

11. 对称加密（对称加密）

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

需要对加密和解密使用相同密钥的加密算法。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用。对称性加密也称为密钥加密。

所谓对称，就是采用这种加密方法的双方使用方式用同样的密钥进行加密和解密。密钥是控制加密及解密过程的指令。算法是一组规则，规定如何进行加密和解密。

因此加密的安全性不仅取决于加密算法本身，密钥管理的安全性更是重要。因为加密和解密都使用同一个密钥，如何把密钥安全地传递到解密者手上就成了必须要解决的问题。

对称加密算法：DES、DESede、AES、IDEA、PBE 等。

12. 非对称加密（非对称加密）

对称加密算哒在密钥和解密时使用的是同一个密钥；而非对称加密算法需要两个密钥来进行加密和解密，这两个密钥是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥）。

非对称密码算法：RSA、Elgamal、背包算法、Rabin、D-H、ECC 等。

13. 加密机（加密机）

加密机是通过国家商用密码主管部门鉴定并批准使用的国内自主开发的主机加密设备，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。

加密机功能模块：硬件加密部件、密钥管理菜单、加密机后台进程、加密机监控程序和后台监控进程等。

14. 嗅探（嗅探）

嗅探计算机网络的共享通讯隧道的，支持每对通讯计算机独占通道的交换机/集线器仍然过于昂贵，共享意为着计算机能够接收到发送给其他计算机的信息，捕获在网络中传输的数据信息就称为嗅探。

一般指嗅探器，嗅探器可以获取网络上流经的数据包。

用集线器 hub 组建的网络是基于共享的原理的， 局域网内所有的计算机都接收相同的数据包， 而网卡构造了硬件的"过滤器"通过识别 MAC 地址过滤掉和自己无关的信息。

嗅探程序只需关闭这个过滤器， 将网卡设置为"混杂模式"就可以进行嗅探 用交换机 switch 组建的网络是基于"交换"原理的 ，交换机不是把数据包发到所有的端口上， 而是发到目的网卡所在的端口。

简单来说：嗅探就是窃听网络上流经的数据包。

15. 探针（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。

探针卡是一种测试接口，主要对裸芯进行测试，通过连接测试机和芯片，通过传输信号对芯片参数进行测试.。

2019 年曝光的 WiFi 探针技术,甚至无需用户主动连接 WiFi 即可捕获个人信息。

简单来说：探针就是一种信号传输探测工具。

16. 跳板（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，控制其他主机，一般和肉鸡连用。

目的：就是为了隐藏自己的地址，让别人无法查找到自己的位置。

简单原理：

举个例子，你在 A 朋友家玩儿，发现了通往 B 朋友家的后门，然后你来到了 B 朋友家，又发现了 C 朋友家的厨房是和 B 朋友家相连的，你就顺便来到了 C 朋友的家，同时 C 朋友家的厕所又是和 D 朋友家相连。

你在 A 朋友家做了一些事情，比如设置和修改。

A 朋友回家了，他会发现有人进了自己的家，但是他顺着路线可以找到 B 朋友家，通过长期的寻找，终于找到了 C 朋友家，但他遇见难题了，他并不知道是 B 朋友家的人动了自己的东西，还是 D 朋友家的人动了自己的东西。这时，你就是安全的了。

这中间的各种朋友关系，其实就是你的跳板。

通过这种跳板的转换，我们可以改变自己上网的 IP 位置，隐藏自己的真实物理位置。

17. RARP（RARP）

反向地址转换协议（RARP：Reverse Address Resolution Protocol）反向地址转换协议（RARP）允许局域网的物理机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。

网络管理员在局域网网关路由器里创建一个表以映射物理映射表（MAC）和与其对应的 IP 地址。

当设置一台新的机器时，其 RARP 客户机程序需要向路由器上的 RARP 服务器请求相应的 IP 地址。

假设在路由表中已经设置了一个记录，RARP 服务器将会返回 IP 地址给机器，此机器就会存储起来以便日后使用。

RARP 可以使用于以太网、光纤分布式数据接口及令牌环 LAN 等。

简单来说：RARP 就是将硬件地址映射到网络地址一种协议。

18. UDP（UDP）

internet 协议集支持一个无连接的传输协议，该协议称为用户数据包协议（UDP，User Datagram Protocol）。

UDP 为应用程序提供了一种无需建立连接就可以发送封装的 IP 数据包的方法。RFC 768

描述了 UDP。

Internet 的传输层有两个主要协议，互为补充。无连接的是 UDP，它除了给应用程序发送数据包功能并允许它们在所需的层次上架构自己的协议之外，几乎没有做什么特别的事情。面向连接的是 TCP，该协议几乎做了所有的事情。

简单来说：UDP 是 UserDatagram Protocol 的简称，中文名是用户数据报协议，是 OSI 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

19. TCP（TCP）

传输控制协议（TCP，Transmission Control Protocol）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由 IETF 的 RFC 793 定义。

TCP 旨在适应支持多网络应用的分层协议层次结构。 连接到不同但互连的计算机通信网络的主计算机中的成对进程之间依靠 TCP 提供可靠的通信服务。TCP 假设它可以从较低级别的协议获得简单的，可能不可靠的数据报服务。 原则上，TCP 应该能够在从硬线连接到分组交换或电路交换网络的各种通信系统之上操作。

简单来说：TCP 就是一种面向连接的、可靠的、基于字节流的传输层通信协议

20. FTP（FTP）

文件传输协议（File Transfer Protocol，FTP）是用于在网络上进行文件传输的一套标准协议，它工作在 OSI 模型的第七层， TCP 模型的第四层， 即应用层， 使用 TCP 传输而不是 UDP，客户在和服务器建立连接前要经过一个"三次握手"的过程， 保证客户与服务器之间的连接是可靠的， 而且是面向连接，为数据传输提供可靠保证。

FTP 允许用户以文件操作的方式（如文件的增、删、改、查、传送等）与另一主机相互通信。然而， 用户并不真正登录到自己想要存取的计算机上面而成为完全用户， 可用 FTP 程序访问远程资源， 实现用户往返传输文件、目录管理以及访问电子邮件等等， 即使双方计算机可能配有不同的操作系统和文件存储方式。

简单来说：就是允许用户以文件操作的方式（文件的增、删、改、查、传送等）与另一主机相互通信的传输层的一种协议。

21. SNTP（SNTP）

简单网络时间协议（Simple Network Time Protocol），由 NTP 改编而来，主要用来同步因特网中的计算机时钟。在 RFC2030 中定义。

22. SMTP（SMTP）

SMTP 是一种提供可靠且有效的电子邮件的协议。

SMTP 是建立在 FTP 文件传输服务上的一种邮件服务，主要用于系统之间的邮件信息传递，并提供有关来信的通知。

SMTP 独立于特定的传输子系统，且只需要可靠有序的数据流信道支持，SMTP 的重要特性之一是其能跨越网络传输邮件，即"SMTP 邮件中继 "。

使用 SMTP，可实现相同网络处理进程之间的邮件传输，也可通过中继网或网关实现某处理进程与其他网络之间的邮件传输。

简单来说：SMTP 就是为系统之间传送电子邮件的一种协议。

23. TELNET（TELNET）

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。

它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 telnet 程序，用它连接到服务器。

终端使用者可以在 telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个 telnet 会话，必须输入用户名和密码来登录服务器。Telnet 是常用的远程控制 Web 服务器的方法。

简单来说：TELNET 就是允许用户以虚终端方式访问远程主机的一种协议。

24. HTTP（HTTP）

超文本传输协议（HypertextTransferProtocol，HTTP）是一个简单的请求-响应协议，它通常运行在 TCP 之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。

请求和响应消息的头以 ASCLL 形式给出；而消息内容则具有一个类似 MIME 的格式。

这个简单模型是早期 web 成功的有功之臣，因为它使开发和部署非常地直截了当。

简单来说：HTTP 就是应用层的一个请求响应的协议。

25. HTTPS（HTTPS）

HTTPS （全称：Hyper Text Transfer Protocol over SecureSocket Layer），是以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性。

HTTPS 在 HTTP 的基础下加入 SSL，HTTPS 的安全基础是 SSL，因此加密的详细内容就需要 SSL。

HTTPS 存在不同于 HTTP 的默认端口及一个加密/身份验证层（在 HTTP 与 TCP 之间）。

这个系统提供了身份验证与加密通讯方法。它被广泛用于 万维网上安全敏感的通讯，例如交易支付等方面。

简单来说：HTTP 就是应用层的一个加密的请求响应的协议。

[渗透入门篇] 渗透行业必备术语大集合(六)

ICMP、DNS、CDN、TCP/IP、OSI

LAN、MAN、WAN、EXP、POC

payload、shellcode、HTML、CSS、Javascript

CMS、VPS、源损耗、域名、URL

cURL、URI、URN、CTF、AWD

1. ICMP（ICMP）

ICMP（Internet Control Message Protocol）Internet 控制报文协议。

它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。

控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。

这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ICMP 使用 IP 的基本支持，就像它是一个更高级别的协议，但是，ICMP 实际上是 IP 的一个组成部分，必须由每个 IP 模块实现。

"ICMP 协议"对于网络安全有着极其重要的意义，其本身的特性决定了它非常容易被用于攻击网络上的路由器和主机。

例如，曾经轰动一时的海信主页被黑事件就是以 ICMP 攻击为主的。由于操作系统规定 ICMP 数据包最大尺寸不超过 64KB，因而如果向目标主机发送超过 64KB 上限的数据包，该主机就会出现内存分配错误，进而导致系统耗费大量的资源处理，疲于奔命，最终瘫痪、死机。

2. DNS（DNS）

域名系统（英文：Domain Name System：DNS）是互联网的一项服务。

它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。

DNS 使用 UDP 端口 53。

当前，对于每一级域名长度的限制是 63 个字符，域名总长度则不能超过 253 个字符。

简单来叔：DNS 协议就是用来将域名解析到 IP 地址的一种协议，当然，也可以将 IP 地址转换为域名的一种协议这个就是拥有 CDN 的网站，想找到真实 ip 地址，需要绕过 CDN。

3. CDN（CDN）

CDN 的全称是 Content Delivery Network，即内容分发网络。

CDN 是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。

CDN 的关键技术主要有内容存储和分发技术。

基本原理：

广泛采用各种缓存服务器，将这些缓存服务器分布到用户访问相对集中的地区或网络中，在用户访问网站时，利用全局负载技术将用户的访问指向距离最近的工作正常的缓存服务器上，由缓存服务器直接响应用户请求。

主要功能：

(1)节省骨干网带宽，减少带宽需求量；

(2)提供服务器端加速，解决由于用户访问量大造成的服务器过载问题；

(3)服务商能使用 Web Cache 技术在本地缓存用户访问过的 Web 页面和对象，实现相同对象的访问无须占用主干的出口带宽，并提高用户访问因特网页面的相应时间的需求；

(4)能克服网站分布不均的问题，并且能降低网站自身建设和维护成本；

(5)降低“通信风暴”的影响，提高网络访问的稳定性。

4. TCP/IP（TCP/IP）

TCP/IP 传输协议，即传输控制/网络协议，也叫作网络通讯协议，是在网络的使用中的最基本的通信协议。

TCP/IP 传输协议对互联网中各部分进行通信的标准和方法进行了规定。

TCP/IP 传输协议是保证网络数据信息及时、完整传输的两个重要的协议。

TCP/IP 传输协议是严格来说是一个四层的体系结构，应用层、传输层、网络层和数据链路层都包含其中。

四层：

1. 应用层的主要协议有 telnet、FTP、SMTP 等，是用来接收来自传输层的数据或者按不同应用要求与方式将数据传输至传输层。

2. 传输层的主要协议有 UDP、TCP，是使用者使用平台和计算机信息网内部数据结合的通道，可以实现数据传输与数据共享。

3. 网络层的主要协议有 ICMP、IP、IGMP，主要负责网络中数据包的传送等。

4. 网络访问层，也叫网路接口层或数据链路层，主要协议有 ARP、RARP，主要功能是提供链路管理错误检测、对不同通信媒介有关信息细节问题进行有效处理等。

5. OSI（OSI）

意为开放式系统互联，国际标准化组织制定了 OSI（Open System Interconnection）模型。

这个模型把网络通信的工作分为 7 层，分别是物理层，数据链路层，网络层，传输层，会话层，表示层和应用层。

1 至 4 层被认为是低层，这些层与数据移动密切相关。

5 至 7 层是高层，包含应用程序级的数据。

每一层负责一项具体的工作，然后把数据传送到下一层。

具体的介绍可以查看链接。

6. LAN（LAN）

局域网，网络种类，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。

简单来说：局域网就是一种网络，连接近距离的计算机，一般位于单个房间、建筑物或小的地理区域里。LAN 上的所有系统位于一个网络跳之间

7. MAN（MAN）

全称 Metropolitan Area Network，即城域网。

是在一个城市范围内所建立的计算机通信网，属宽带局域网。

由于采用具有有源交换元件的局域网技术，网中传输延时较小，它的传输媒介主要采用光缆，传输速率在 100 兆比特/秒以上。

MAN 的一个重要用途是用作骨干网，通过它将位于同一城市内不同地点的主机、数据库，以及 LAN 等互相联接起来，这与 WAN 的作用有相似之处，但两者在实现方法与性能上有很大差别。

基于一种大型的 LAN，通常使用与 LAN 相似的技术。

MAN 单独的列出的一个主要原因是已经有了一个标准：分布式队列双总线 DQDB（Distributed Queue Dual Bus），即 IEEE802.6。

DQDB 是由双总线构成，所有的计算机都连结在上面。

8. WAN（WAN）

广域网（英语：Wide Area Network，缩写为 WAN），又称**外网**、**公网**。和我们前面讲的公网、外网是一个概念。

是连接不同地区局域网或城域网计算机通信的远程网。

通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个地区、城市和国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。广域网并不等同于互联网。

9. EXP（EXPloit）

Exploit 的英文意思就是利用，它在黑客眼里就是漏洞利用。

有漏洞不一定就有 Exploit（利用），有 Exploit 就肯定有漏洞。

我们几乎每隔几天就能听到最近有一个新发现的可以被利用(exploit)的漏洞(vulnerability)，然后给这个漏洞打上补丁。

而事实上，这里面的内容比你想象的要多，因为你不可能知道所有软件的漏洞，而且那些可利用的漏洞也只是被少数人所了解。

简单来说：就是漏洞利用代码，运行之后对目标进行攻击。

10. POC（Proof of Concept）

概念证明，即**概念验证**（英语：Proof of concept，简称 POC）是对某些想法的一个较短而不完整的实现，以证明其可行性，示范其原理，其目的是为了验证一些概念或理论。

概念验证通常被认为是一个有里程碑意义的实现的原型 。

在计算机安全术语中，**概念验证**经常被用来作为 0day、exploit 的别名。

简单来说：漏洞验证代码，检测目标是否存在对应漏洞。

11. payload（payload）

病毒通常会做一些有害的或者恶性的动作。

在病毒代码中实现这个功能的部分叫做"有效负载"（payload）。

payload 可以实现任何运行在受害者环境中的程序所能做的事情，并且能够执行动作包括破坏文件删除文件，向病毒的作者或者任意的接收者发送敏感信息，以及提供通向被感染计算机的后门。

简单来说：就是指成功 exploit 之后，真正在目标系统执行的代码或指令。

12. shellcode（shellcode）

shellcode 是一段用于利用软件漏洞而执行的代码，shellcode 为 16 进制的机器码，因为经常让攻击者获得 shell 而得名。

shellcode 常常使用机器语言编写。

可在暂存器 eip 溢出后，塞入一段可让 CPU 执行的 shellcode 机器码，让电脑可以执行攻击者的任意指令。

Shellcode：简单翻译'shell 代码'，是 Payload 的一种，由于其建立正向/反向 shell 而得名。

13. HTML（HTML）

HTML（HyperTextMarkup Language）的全称为超文本标记语言，是一种标记语言。

它包括一系列标签，通过这些标签可以将网络上的文档格式统一，使分散的 internet 资源连接为一个逻辑整体。

HTML 文本是由 HTML 命令组成的描述性文本，HTML 命令可以说明文字，图形、动画、声音、表格、连接等。

超文本是一种组织信息的方式，它通过超级链接方法将文本中的文字、图表与其他信息媒体相关联。

这些相互关联的信息媒体可能在同一文本中，也可能是其他文件，或是地理位置相距遥远的某台计算机上的文件。

这种组织信息方式将分布在不同位置的信息资源用随机方式进行连接，为人们查找，检索信息提供方便。

简单来说：HTML 是一种用于创建网页的标准标记语言，您可以使用 HTML 来建立自己的 WEB 站点，HTML 运行在浏览器上，由浏览器来解析。

14. CSS（CSS）

层叠样式表(英文全称：CascadingStyleSheets)是一种用来表现 HTML（标准通用标记语言的一个应用）或 XML（标准通用标记语言的一个子集）等文件样式的计算机语言。CSS 不仅可以静态地修饰网页，还可以配合各种脚本语言动态地对网页各元素进行格式化。

CSS 能够对网页中元素位置的排版进行像素级精确控制，支持几乎所有的字体字号样式，拥有对网页对象和模型样式编辑的能力。

15. Javascript（Javascript）

JavaScript（简称“JS”） 是一种具有函数优先的轻量级，解释型或即时编译型的编程语言。

虽然它是作为开发 web 页面的脚本语言而出名，但是它也被用到了很多非浏览器环境中，JavaScript 基于原型编程、多范式的动态脚本语言，并且支持面向对象、命令式、声明式、函数时式编程范式。

JavaScript 是一种属于网络的高级脚本语言,已经被广泛用于 Web 应用开发,常用来为网页添加各式各样的动态功能，为用户提供更流畅美观的浏览效果。

通常 JavaScript 脚本是通过嵌入在 HTML 中来实现自身的功能的。

16. CMS（内容管理系统）

内容管理系统（content management system，CMS），是一种位于 WEB 前端（Web 服务器）和后端办公系统或流程（内容创作、编辑）之间的软件系统。

内容的创作人员、编辑人员、发布人员使用内容管理系统来提交、修改、审批、发布内容。

这里指的"内容"可能包括文件、表格、图片、数据库中的数据甚至视频等一切你想要发布到 Internet、internet 以及 exteanet 网站的信息。

内容管理还可选地提供内容抓取工具，将第三方信息来源，比如将文本文件、HTML 网页、Web 服务、关系数据库等的内容自动抓取，并经分析处理后放到自身的内容库中。

随着个性化的发展，内容管理还辅助 WEB 前端将内容以个性化的方式提供给内容使用者，即提供个性化的门户框架，以基于 WEB 技术将内容更好地推送到用户的浏览器端。

内容管理系统是企业信息化建设和电子政务的新宠，也是一个相对较新的市场。对于内容管理，业界还没有一个统一的定义，不同的机构有不同的理解。

17. VPS（VPS）

VPS（Virtual Private Server 虚拟专用服务器）技术，将一台服务器分割成多个虚拟专享服务器的优质服务。实现 VPS 的技术分为容器技术，和虚拟化技术。在容器或虚拟机中，每个 VPS 都可选配独立公网 IP 地址、独立操作系统、实现不同 VPS 间磁盘空间、内存、CPU 资源、进程和系统配置的隔离，为用户和应用程序模拟出“独占”使用计算资源的体验。VPS 可以像独立服务器一样，重装操作系统，安装程序，单独重启服务器。VPS 为使用者提供了管理配置的自由，可用于企业虚拟化，也可以用于 IDC 资源租用。

IDC 资源租用，由 VPS 提供商提供。不同 VPS 提供商所使用的硬件 VPS 软件的差异，及销售策略的不同，VPS 的使用体验也有较大差异。尤其是 VPS 提供商超卖，导致实体服务器超负荷时，VPS 性能将受到极大影响。相对来说，容器技术比虚拟机技术硬件使用效率更高，更易于超卖，所以一般来说容器 VPS 的价格都高于虚拟机 VPS 的价格。

这些 VPS 主机以最大化的效率共享硬件、软件许可证以及管理资源。每个 VPS 主机都可选配独立公网 IP 地址、独立操作系统、独立超大空间、独立内存、独立 CPU 资源、独立执行程序和独立系统配置等。VPS 主机用户除了可以分配多个虚拟主机及无限企业邮箱外， 更具有独立主机功能，可自行安装程序，单独重启或重装主机（部分虚拟化/容器技术不支持更换内核）。

简单来说：VPS 就是通过虚拟化技术隔离出来的系统。VPS 主机是一项服务器虚拟化和自动化技术，它采用的是操作系统虚拟化技术。

18. 源损耗（损耗）

损耗，一般指损失，受损失或耗费的意思。这里指的是 VPS 的损耗。

VPS 操作系统虚拟化的概念是基于共用操作系统内核，这样虚拟服务器就无需额外的虚拟化内核的过程，因而虚拟过程资源损耗就更低，从而可以在一台物理服务器上实现更多的虚拟化服务器。

19. 域名（域名）

域名（英语：DomainName），又称网域，是由一串用点分隔的名字组成的 Internet 上某一台计算机或计算机组的名称，用于在数据传输时对计算机的定位标识（有时也指地理位置）。

由于 IP 地址具有不方便记忆并且不能显示地址组织的名称和性质等缺点，人们设计出了域名，并通过网域名称系统（DNS，Domain Name System）来将域名和 IP 地址相互映射，使人更方便地访问互联网，而不用去记住能够被机器直接读取的 IP 地址数串。

20. url（统一资源定位符）

URL 全称：uniform resource locator，即统一资源定位系统。

url 是以太网的万维网服务程序上用于指定信息位置的表示方法。

它最初是由蒂姆·伯纳斯·里发明用来作为万维网的地址。现在它已经被万维网联盟编制为互联网标准 RFC1738。

21. URI（统一资源标识符）

URI 全称：Uniform Resource Identifier，即统一资源标识符。

是一个用于标识某一互联网资源名称的字符串。

该种标识允许用户对任何（包括本地和互联网）的资源通过特定的协议进行交互操作。URI 由包括确定语法和相关协议的方案所定义。

Web 上可用的每种资源，如 HTML、文档、图像、视频片段、程序等，由一个通用资源标识符（Uniform Resource Identifier, 简称"URI"）进行定位。

22. URN（统一资源名称）

URN 全称：Uniform Resource Name，即统一资源名称，是带有名字的因特网资源。

URN 是统一资源标识（URI）的历史名字，它使用 urn：作为 URI scheme。

23. curl（curl）

cURL 是一个利用 URL 语法在命令行下工作的文件传输工具，1997 年首次发行。它支持文件上传和下载，所以是综合传输工具，但按传统，习惯称 cURL 为下载工具。cURL 还包含了用于程序开发的 libcurl。

cURL 支持的通信协议：FTP、FTPS、HTTP、HTTPS、TFTP、SFTP、Gopher、SCP、tenlent、DICT、FILE、LDAP、LDAPS、IMAP、POP3、SMTP 和 RTSP。

curl 还支持 SSL 认证、HTTP POST、HTTP PUT、FTP 上传，HTTP form based upload、proxies、HTTP/2、cookies、用户名+密码认证(Basic，Plain，Digest，CRAM-MD5，NTLM，Negotiate and Kerberos)、file transfer resume、proxy tunneling。

24. CTF（CTF）

CTF（CaptureThe Flag）中文一般译作夺旗赛，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 起源于 1996 年 DEFCON 全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。

已经成为全球范围网络安全圈流行的竞赛形式，2013 年全球举办了超过五十场国际性 CTF 赛事。

而 DEFCON 作为 CTF 赛制的发源地，DEFCON CTF 也成为了全球最高技术水平和影响力的 CTF 竞赛，类似于 CTF 赛场中的"世界杯"。

CTF 竞赛模式具体分为以下三类：

1. 解题模式（Jeopardy）

2. 攻防模式（Attack-Defense）

3. 混合模式（Mix）

25. AWD（AWD）

AWD(AttackWithDefense，攻防兼备)，CTF 的模式之一。

在攻防模式 CTF 赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

攻防模式 CTF 赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。

在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续 48 小时及以上），同时也比团队之间的分工配合与合作。

这个模式是一个非常有意思的模式，你需要在一场比赛里要扮演攻击方和防守方，攻者得分，失守者会被扣分。

也就是说，攻击别人的靶机可以获取 Flag 分数时，别人会被扣分，同时你也要保护自己的主机不被别人得分，以防扣分。

[渗透入门篇] 渗透行业必备术语大集合(七)

CVE、SRC、CNVD、0day、1day

Nday、C2、横移、暴库、CA 证书

数字证书、SSL 证书、数字签名、漏扫、UTM

网闸、数据库审计、DLP、SD-WAN、SOC

SIEM、MIME、沙箱、沙箱逃逸、网络靶场

---

1. CVE（CVE）

CVE 全称：Common Vulnerabilities & Exposures，即通用漏洞披露。

CVE 就好像是一个字典表，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称。

使用一个共同的名字，可以帮助用户在各自独立的各种漏洞数据库中和漏洞评估工具中共享数据，虽然这些工具很难整合在一起。

这样就使得 CVE 成为了安全信息共享的"关键字"。

如果在一个漏洞报告中指明的一个漏洞，如果有 CVE 名称，你就可以快速地在任何其它 CVE 兼容的数据库中找到相应修补的信息，解决安全问题。

2. SRC（SRC）

全称：Security Emergency Response Center，即安全应急响应的中心

主要针对科技互联网企业常见的安全漏洞而特别设立的机构。

3. CNVD（国家信息安全漏洞共享平台）

CNVD 全称：China National Vulnerability Database，即国家信息安全漏洞共享平台。

是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，简称 CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

建立 CNVD 的主要目标即与国家政府部门、重要信息系统用户、运营商、主要安全厂商、软件厂商、科研机构、公共互联网用户等共同建立软件安全漏洞统一收集验证、预警发布及应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，进而提高我国信息系统及国产软件的安全性，带动国内相关安全产品的发展。

4. 0day（0day）

0day 在网络安全界通常是指没有补丁的漏洞利用程序，提供该利用程序的人通常是该漏洞的首发者或是第一个公开该漏洞利用细节的人。

网络安全意思上的 0day 就是指一些没有公布补丁的漏洞，或者是还没有被漏洞发现者公布出来的漏洞利用工具，由于这种漏洞的利用程序对网络安全都具有巨大威胁，因此 0day 也成为黑客的最爱。一般的黑客软件带有 0day 的名字指的是此漏洞还没有打补丁而软件已经公布。

目前国内 0day 的地下交易已经比较成熟，对 0day 有需求的包括大型的网络安全公司比如 iDefence，职业黑客。

提供 0day 的一般都是漏洞研究爱好者或是比较松散的网络安全组织,可以参考国外的 0day 研究网站。某些外国网站的发布的作品可能就是中国人做的呢！！

5. 1day（1day）

1day 就是刚公布后的漏洞，或者公布后没有 poc exp 的漏洞。或者指刚公布一天的漏洞，大部分通杀。

已被发现官方刚发布补丁网络上还大量存在的 Vulnerability。

6. Nday（Nday）

Nday 就是公布很久，流传很广的漏洞，少数不更新的才能用。相对来说，通杀性不高。

7. C2（C2）

As the name itself suggests, command-and-control (C&C) servers are used to remotely send often malicious commands to a botnet, or a compromised network of computers. The term originated from the military concept of a commanding officer directing control to his/her forces to accomplish a goal. C&C servers were popular for using
internet relay chat (IRC) networks, legitimate websites, and dynamic DNS services. The backdoor malware, BKDR_ MAKADOCS .JG, is noted for its evasion technique against anti-malware as it uses Google Docs for its C&C communication.

顾名思义，命令与控制（C&C）服务器被用来向僵尸网络或受损的计算机网络远程发送恶意命令。该术语源自军事概念，即指挥官将控制权交给他/她的部队以实现目标。C&amp；C（控制）服务器很受欢迎 internet 中继聊天（IRC）网络、合法网站和动态 DNS 服务。后门恶意软件，BKDR_uuMakadocs.JG 以其规避反恶意软件的技术而闻名。

C2 全称为 Command and Control，即命令与控制，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”

8. 横移（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。

9. 暴库（暴库）

就是通过一些技术手段或者程序漏洞得到数据库的地址，并将数据非法下载到本地。

黑客非常乐意于这种工作，为什么呢？

因为黑客在得到网站数据库后，就能得到网站管理账号，对网站进行破坏与管理，黑客也能通过数据库得到网站用户的隐私信息，甚至得到服务器的最高权限。

简单来说：就是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，通常都用于 SQL 注入。

10. CA 证书（CA 证书）

CA 是证书的签发机构，它是公钥基础设施（Public Key Infrastructure，PKI）的核心。

CA 是负责签发证书、认证证书、管理已颁发证书的机关。CA 拥有一个证书（内含公钥和私钥）。

网上的公众用户通过验证 CA 的签字从而信任 CA ，任何人都可以得到 CA 的证书（含公钥），用以验证它所签发的证书。

如果用户想得到一份属于自己的证书，他应先向 CA 提出申请。

在 CA 判明申请者的身份后，便为他分配一个公钥，并且 CA 将该公钥与申请者的身份信息绑在一起，并为之签字后，便形成证书发给申请者。

如果一个用户想鉴别另一个证书的真伪，他就用 CA 的公钥对那个证书上的签字进行验证，一旦验证通过，该证书就被认为是有效的。证书实际是由证书签证机关（CA）签发的对用户的公钥的认证。

证书的内容包括：电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等等。证书的格式和验证方法普遍遵循 X.509 国际标准。

简单来说：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。

11. 数字证书（数字证书）

数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。

因此数字证书又称为数字标识。数字证书对网络用户在计算机网络交流中的信息和数据等以加密或解密的形式保证了信息和数据的完整性和安全性。

12. SSL 证书（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。

SSL 证书就是遵守 SSL 协议，由受信任的数字证书颁发机构 CA，在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能。

13. 数字签名（数字签名）

数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

它是一种类似写在纸上的普通的物理签名，但是在使用了公钥领域的技术来实现的，用于鉴别数字信息的方法。

一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。数字签名是非对称密钥加密技术与摘要算法技术的应用。

14. 漏扫（漏洞扫描）

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。

漏洞扫描器包括网络漏扫、主机漏扫、数据库漏扫等不同种类。

15. UTM（UTM）

UTM 全称：UnifiedThreatManagement，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。

16. 网闸（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，使系统间不存在通信的物理连接、逻辑连接及信息传输协议，不存在依据协议进行的信息交换，而只有以数据文件形式进行的无协议摆渡。

因此，网闸从物理上隔离、阻断了对内网具有潜在攻击可能的一切网络连接，使外部攻击者无法直接入侵、攻击或破坏内网，保障了内部主机的安全。

17. 数据库审计（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。

数据库审计是数据库安全技术之一，数据库安全技术主要包括：数据库漏洞扫描、数据库加密、数据库防火墙、数据脱敏、数据库安全审计系统。

黑客的 SQL 注入攻击行为，可以通过数据库审计发现。

18. DLP（数据防泄漏）

当前我国涉及部门(军队、军工、政府、金融行业、保险行业、电信行业等)中，80%以上应用系统使用国外数据库产品，特别是 Oracle；如何保证系统在高性能、高可用的同时提升数据的安全性，确保关键信息不被泄露、国家利益不受损失已经迫在眉睫。

数据防泄漏可以通过数据库加密实现核心数据加密存储，可以通过数据库防火墙实现批量数据泄漏的网络拦截，也可以通过数据脱敏实现外发敏感数据的匿名化，这些数据库安全技术可以实现数据防泄漏问题。

简单来说：DLP 就是数据防泄漏，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。

19. SD-WAN（SD-WAN）

SD-WAN 全称 Software Defined Wide Area Network，即软件定义广域网，是将 SDN 技术应用到广域网场景中所形成的一种服务，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’，支持应用可感知的网络能力开放。

20. SOC（SOC）

SOC 全称：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

21. SIEM（SIEM）

SIEM 全称：security information and event management，即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。

22. MIME（MIME）

MIME(Multipurpose Internet Mail Extensions)多用途互联网邮件扩展类型。

是设定某种拓展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。

多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。

23. 沙箱（沙箱）

沙箱是一种按照安全策略限制程序行为的执行环境。早期主要用于测试可疑软件等，比如黑客们为了试用某种病毒或者不安全产品，往往可以将它们在沙箱环境中运行。

经典的沙箱系统的实现途径一般是通过拦截系统调用，监视程序行为，然后依据用户定义的策略来控制和限制程序对计算机资源的使用，比如改写注册表，读写磁盘等。

简单来说：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。

24. 沙箱逃逸（沙箱逃逸技术）

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

25. 网络靶场（网络靶场）

网络靶场（Cyber Range）是一种基于虚拟化技术，对真实网络空间中的网络架构、系统设备、业务流程的运行状态及运行环境进行模拟和复现的技术或产品，以更有效地实现与网络安全相关的学习、研究、检验、竞赛、演习等行为，从而提高人员及机构的网络安全对抗水平。

网络靶场包含了在线网络攻防学习环境、网络安全赛事平台、网络安全技术测评研究平台，城市级甚至国家级的网络攻防演练平台等，都可以归属于网络靶场的概念。然而，在这些可以被称为网络靶场的产品中，也存在很大的差异：支持规模的量级差异、模拟环境的复杂程度、各行业应用场景的不同、网络靶场对现实的复现程度（即仿真程度）等等。

网络靶场作为支撑网络空间安全技术验证、网络武器装备试验、攻防对抗演练和网络风险评估的重要基础设施，成为新兴网络安全战略、专业人才队伍建设的重要支撑手段。

简单来说：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。

[渗透入门篇] 渗透行业必备术语大集合(八)

黑名单、白名单、南北向流量、东西向流量、大数据安全分析

杀伤链、网络空间测绘、逆向、防爬、安全资源池

区块链、安全众测、代码审计、数据脱敏、箱子

漏洞复现、软件木马、脚本木马、3899 肉鸡、4899 肉鸡

缓冲区溢出、嗅探器、CMD、powershell、常见端口

---

1. 黑名单（黑名单）

在网络 SEO 优化当中，搜索引擎或者义务用户收集的搜索引擎垃圾制造者列表，可以用于从搜索引擎封杀这些垃圾制造者，或者抵制他们。

简单来说：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。

2. 白名单（白名单）

白名单的概念与"黑名单"相对应。

例如：在电脑系统里，有很多软件都应用到了黑白名单规则，操作系统、防火墙、杀毒软件、邮件系统、应用软件等，凡是涉及到控制方面几乎都应用了黑白名单规则。

简单来说：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.

3. 南北向流量

通常指数据中心内外部通信所产生的的流量。

4. 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。

5. 大数据安全分析（大数据分析）

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。

6. 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 KillChain，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。

7. 网络空间测绘（网络空间测绘）

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。

网络空间测绘，在国家把网络空间安全概念提升到一个重要的层次时，更显重要。因为要搞网络攻防，首先得了解网络，要了解网络空间，就需要对网络空间测绘。

简单来说：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

8. 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。

9. 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。

10. 安全资源池（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。

11. 区块链（区块链）

英文名为 blockchain。

区块链是一个信息技术领域的术语。从本质上讲，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。

基于这些特征，区块链技术奠定了坚实的“信任”基础，创造了可靠的“合作”机制，具有广阔的运用前景。

12. 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。

13. 代码审计（代码审计）

代码审计（Code audit）是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析。软件代码审计是对编程项目中源代码的全面分析，旨在发现错误，安全漏洞或违反编程约定。 它是防御性编程范例的一个组成部分，它试图在软件发布之前减少错误。

C 和 C ++源代码是最常见的审计代码，因为许多高级语言（如 Python）具有较少的潜在易受攻击的功能（例如，不检查边界的函数）。

简单来说：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。

14. 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。

在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如身份证号、手机号、卡号、客户号等个人信息都需要进行数据脱敏。

简单来说：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。

15. 箱子

箱子就是别人通过将木马挂在网页上，然后别人点击了这个网页后就中了木马，登陆游戏后木马就会记录这个人的游戏帐号密码，然后发到挂木马这个人的指定的一个地方。

这个地方就叫游戏箱子。

16. 漏洞复现

你发现了一个漏洞你需要将这个漏洞展示出来。

17. 软件木马

远控软件的被控端（exe 文件）。

18. 脚本木马

脚本语言编写的被控端（asp、php…）

19. 3389 肉鸡

3389 是 WINDWS 终端服务（Terminal Services）所默认使用的端口号，该服务是微软为了方便网络管理员远程管理及维护服务器而推出的，网络管理员可以使用远程桌面连接到网络上任意一台开启了终端服务的计算机上，成功登陆后就会象操作自己的电脑一样来操作主机了。

这和远程控制软件甚至是木马程序实现的功能很相似，终端服务的连接非常稳定，而且任何杀毒软件都不会查杀，所以也深受黑客喜爱。黑客在拿下了一台主机后，通常都会想办法先添加一个属于自己的后门帐号，然后再开启对方的终端服务，这样，自己就随时可以使用终端服务来控制对方了，这样的主机，通常就会被叫做 3389 肉鸡。

20. 4899 肉鸡

Radmin 是一款非常优秀的远程控制软件，4899 就是 Radmin 默认使以也经常被黑客当作木马来使用（正是这个原因，目前的杀毒软件也对 Radmin 查杀了）。

有的人在使用的服务端口号。

因为 Radmin 的控制功能非常强大，传输速度也比大多数木马快，而且又不被杀毒软件所查杀，所用 Radmin 管理远程电脑时使用的是空口令或者是弱口令，黑客就可以使用一些软件扫描网络上存在 Radmin 空口令或者弱口令的主机，然后就可以登陆上去远程控制对恶劣，这样被控制的主机通常就被成做 4899 肉鸡。

21. 缓冲区溢出

功击者向一个地址区输入这个区间存储不下的大量字符。

在某些性况下，这些多余的字符可以作为"执行代码"来运行，因此足以使功击者不受安全措施限制地获得计算机的控制权。

22. 嗅控器（Snifffer）

就是能够捕获网络报文的设备。

嗅控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。

23. CMD

是一个所谓命令行控制台。有两条进入该程序的通道：

第一、鼠标点击"开始—运行"，在出现的编辑框中键入"CMD"，然后点击"确定"；

第二、在启动 Windows2000 的时候，按 F8 进入启动选择菜单，移动光条或键入数字至安全模式的命令行状态。

出现的窗口是一个在 win9x 系统常见的那种 MSDOS 方式的界面。

尽管微软把这个工具当做命令解释器一个新的实例，但使用方法去和原来的 DOS 没有区别。

24. powershell(windows power shell)

Windows PowerShell 是一种命令行外壳程序和脚本环境，使命令行用户和脚本编写者可以利用 .NET Framework 的强大功能。

它引入了许多非常有用的新概念，从而进一步扩展了您在 Windows 命令提示符和 Windows Script Host 环境中获得的知识和创建的脚本。

Windows PowerShell v3 将伴随着 Microsoft Hyper-V3.0 和 windows server 2012 发布。

PowerShell v3 是一个 Windows 任务自动化的框架，它由一个命令行 shell 和内置在这个.NET 框架上的编程语言组成。

PowerShell v3 采用新的 cmdlet 让管理员能够更深入到系统进程中，这些进程可以制作成可执行的文件或脚本（script）。

一条 cmdlet 是一条轻量命令，Windows PowerShell 运行时间在自动化脚本的环境里调用它。

Cmdlet 包括显示当前目录的 Get-Location，访问文件内容的 Get-Content 和结束运行进程的 Stop-Process。

PowerShell v3 在 Windows Server 8 中装载了 Windows Management Framework 3.0。PowerShell 运行环境也能嵌入到其它应用。

25. 常见端口

- 21 ftp
- 22 SSH
- 23 Telnet
- 80 web
- 80-89 web

- 161 SNMP
- 389 LDAP
- 443 SSL 心脏滴血以及一些 web 漏洞测试
- 445 SMB
- 512,513,514 Rexec
- 873 Rsync 未授权
- 1025,111 NFS
- 1433 MSSQL
- 1521 Oracle:(iSqlPlus Port:5560,7778)
- 2082/2083 cpanel 主机管理系统登陆 （国外用较多）
- 2222 DA 虚拟主机管理系统登陆 （国外用较多）
- 2601,2604 zebra 路由，默认密码 zebra
- 3128 squid 代理默认端口，如果没设置口令很可能就直接漫游内网了
- 3306 MySQL
- 3312/3311 kangle 主机管理系统登陆
- 3389 远程桌面
- 4440 rundeck 参考 WooYun: 借用新浪某服务成功漫游新浪内网
- 5432 PostgreSQL
- 5900 vnc
- 5984 CouchDB http://xxx:5984/_utils/
- 6082 varnish 参考 WooYun: Varnish HTTP accelerator CLI 未授权访问易导致网站被直接篡改或者作为代理进入内网
- 6379 redis 未授权
- 7001,7002 WebLogic 默认弱口令，反序列
- 7778 Kloxo 主机控制面板登录
- 8000-9090 都是一些常见的 web 端口，有些运维喜欢把管理后台开在这些非 80 的端口上
- 8080 tomcat/WDCP 主机管理系统，默认弱口令
- 8080,8089,9090 JBOSS
- 8083 Vestacp 主机管理系统 （国外用较多）
- 8649 ganglia
- 8888 amh/LuManager 主机管理系统默认端口
- 9200,9300 elasticsearch 参考 WooYun: 多玩某服务器 ElasticSearch 命令执行漏洞
- 10000 Virtualmin/Webmin 服务器虚拟主机管理系统
- 11211 memcache 未授权访问
- 27017,27018 Mongodb 未授权访问
- 28017 mongodb 统计页面
- 50000 SAP 命令执行
- 50070,50030 hadoop 默认端口未授权访问
- 554 实时流协议（监控）53 dns 110 pop3 1080 socket5