网络攻击与防范复习

1. 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。

2. ASLR

ASLR（Address Space Layout Randomization）是一种用于增强操作系统安全性的技术，通过随机化进程的内存地址空间布局，使得攻击者无法准确预测目标对象的位置，从而增加攻击者利用漏洞进行攻击的难度

3. botnet

僵尸网络（Botnet）是一种由大量被恶意软件感染的计算机组成的网络，这些计算机被称为“僵尸”或“Bots”

4. chmod

chmod是“change mode”的缩写，主要用于改变文件或目录的访问权限,通过chmod命令，用户可以修改文件或目录的读（r)、写（w）和执行（x）权限，从而控制不同用户对这些资源的访问级别

5. cmd5.com

cmd5.com是一款优秀的在线MD5解密工具，它拥有庞大的数据库，可以快速解密大部分的MD5哈希值。该网站不仅提供基本的解密服务，还支持批量解密和自定义算法等高级功能，以满足各种复杂的需求

6. cookie

Cookie是小型文本文件，设计的初衷是为了辨别用户身份，进行Session追踪而存储在用户客户端的文件。

Cookie本身存在一定的安全隐患，存在Session劫持，XSS攻击等

7. 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

`CreateRemoteThread()` 是一个在 Windows 操作系统中使用的 API 函数，它允许一个进程在其地址空间中创建一个新的线程，以执行另一个进程中的代码。这个函数通常用于调试、进程注入等高级编程任务

8. 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

9. 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。

10.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

11. DEP

Data Execution Prevention，数据执行保护，简称DEP，是一组在存储器上运行额外检查的硬件和软件技术，有助于防止恶意程序码在系统上运行。

12. 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

13. 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

14. DllMain()

`DllMain()` 是 Windows 操作系统中动态链接库（DLL）的入口点函数。这个函数是当 DLL 被加载到进程地址空间、卸载或某个线程附加到或分离于该 DLL 时被系统调用的。它主要用于执行一些初始化或清理工作，比如分配和释放资源、设置线程局部存储（TLS）等。

15. DLP

Data Loss/leak Prevention,数据防泄露工具。

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。

但该类工具普及不多，主要依靠制度防范数据内部泄露，常见的软件有OpenDLP和MyDLP等（见49 OpenDLP，MyDLP）

16. 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。

17. DRM

DRM（Digital Rights Management，数字版权管理）是一种技术手段，旨在保护数字内容的版权和知识产权。它通过对数字内容进行加密、限制使用权限、追踪用户行为等方式，确保内容创作者和分发者能够控制其作品的使用和分发，防止未经授权的复制、分发和滥用。

18. GDPR

GDPR（General Data Protection Regulation，通用数据保护条例）是欧盟（EU）于2016年4月通过、并于2018年5月25日正式生效的一项法规。GDPR旨在加强个人数据的保护，并统一欧盟成员国关于数据保护的法律法规。它不仅适用于欧盟境内的组织，也适用于在欧盟境内处理欧盟公民个人数据的非欧盟组织。

19. 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

20.heartbeat

OpenSSL的heartbeat（心跳）功能是一个用于保持TLS/SSL连接活性的扩展机制

心跳机制主要用于确定连接是否能够正常通信，避免长时间无数据往来而导致的连接自动断开（保活）

21.heartbleed

OpenSSL Heartbleed漏洞是一个严重的安全漏洞，它允许攻击者无需权限即可获取服务器内存中的敏感信息，如私钥、密码等。该漏洞源于OpenSSL心跳扩展（Heartbeat）的逻辑错误，使得攻击者能够通过构造异常数据包获取最多64KB的内存数据。

22. 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。

23. HTTPS

HTTPS是HTTP（HyperText Transfer Protocol，超文本传输协议）的安全版本，通过在HTTP的基础上增加SSL（Secure Sockets Layer，安全套接字层）或TLS（Transport Layer Security，传输层安全性）协议来实现数据的加密传输。这种加密传输方式确保了数据在客户端和服务器之间的传输过程中不会被窃取或篡改。

24. ICAP

ICAP是Internet Content Adaptation Protocol的缩写.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。 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。

25. IDApro

IDA Pro（交互式反汇编器专业版）是一款功能强大的静态反编译工具，由Hex-Rays公司开发。它能够将二进制文件转化为易于阅读和理解的汇编代码，并提供全面的二进制分析功能，包括支持多种处理器架构和文件格式、具有强大的图形化用户界面和插件扩展能力等。IDA Pro被广泛应用于恶意软件分析、漏洞挖掘与修复、软件逆向工程等领域，是逆向工程师和安全研究人员的必备利器。

26. 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。

27. Kerberos

Kerberos是一种计算机网络授权协议，同时也指麻省理工学院（MIT）为这个

协议开发的一套计算机网络安全系统
Kerberos的设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。它能够在非安全网络中，对个人通信以安全的手段进行身份认证。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。

28. Metasploit

Metasploit Framework是一个开源的渗透测试框架。它提供了一组工具和模块，用于进行网络安全测试、漏洞利用和渗透测试。

Metasploit在安全研究、渗透测试和教育领域有着广泛的应用，并且不断更新和改进，以满足不断变化的安全需求。

29. mydlp

MyDLP是一款数据丢失防护（Data Loss Prevention，简称DLP）软件,MyDLP旨在帮助企业识别、监控和保护敏感数据，防止数据泄露和滥用。它通过网络服务器和终端计算机上的多站点配置运行，提供全面的数据丢失防护解决方案。

30. NAS

NAS（Network Attached Storage，网络附属存储）是一种专门的数据存储服务器，它不承担计算任务，只专注于数据存储，并允许网络上的用户通过文件共享协议（如NFS、SMB/CIFS）进行访问。NAS设备通常配备了大容量的硬盘阵列，并内置了操作系统，用于管理数据的存储、备份和恢复等功能。

31. nmap

Network Mapper (Nmap) 是一个网络扫描和主机发现工具。它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，并且可以生成详细的报告。它还可以用于安全评估，帮助识别未修补的漏洞和其他安全问题。Nmap 支持多种操作系统，包括 Windows、Linux 和 macOS。

32. ntop/ntopng

ntopng (ntop next generation)是一个开源网络流量监测工具。它可以收集、分析和报告网络流量数据，包括 IP 协议分布、主机流量、应用程序流量等。

ntopng 还可以用来监测和诊断网络性能问题，并且提供了web 界面和 API 来访问监测数据。 它可以运行在 Linux、Windows 和 macOS 上。

33. O-LLVM

O-LLVM 是一种优化的 LLVM 编译器框架，旨在提高代码生成的性能和效率，通过对中间表示进行多层级的优化，适应特定硬件平台，并支持模块化设计，以实现灵活的优化策略。它的目标是减少运行时开销，提升应用程序的整体性能。

34. ollydbg

Ollydbg 通常称作OD，又叫OllyDebug，是反汇编工作的常用工具。它将IDA与SoftICE结合起来的思想，已代替SoftICE成为当今最为流行的调试解密工具。同时还支持插件扩展功能，是目前最强大的调试工具。

35. PAP

PAP（程序分析与性能）是一种方法论，旨在通过静态和动态分析技术评估程序的性能特征。它关注代码的执行效率、资源使用情况和潜在的性能瓶颈，帮助开发者优化应用程序。PAP 通常结合各种工具和技术，以提供深入的性能分析和改进建议，从而提升软件的整体运行效率。

36. Phishing

Phishing 是一种网络诈骗手段，攻击者通过伪装成可信任的实体（如银行、社交媒体或电子邮件服务）来诱骗用户提供敏感信息，如用户名、密码和信用卡信息。这种攻击通常涉及发送看似合法的电子邮件或创建假网站，以误导用户进行交互，从而窃取其个人信息。Phishing 对用户的网络安全构成严重威胁。

37. PKCS#11

PKCS#11 是一种公钥密码学标准，定义了一个平台独立的接口，用于访问硬件安全模块（HSM）和其他加密设备。它提供了一套标准化的 API，使应用程序能够进行加密、解密、签名和密钥管理等操作。PKCS#11 广泛应用于安全设备和系统中，以确保数据的安全性和完整性，促进跨平台的加密应用开发。

38. RADIUS

RADIUS（远程认证拨号用户服务）是一种网络协议，用于在网络中进行用户身份验证、授权和计费。它主要用于集中管理用户访问，特别是在企业网络和互联网服务提供商中。通过 RADIUS，用户的凭据（如用户名和密码）被发送到 RADIUS 服务器进行验证，从而控制对网络资源的访问。该协议提高了安全性和管理效率，广泛应用于无线网络、VPN 和其他需要身份验证的场景。

39. robots.txt

`robots.txt` 是一种文本文件，用于指导搜索引擎爬虫如何抓取和索引网站的内容。它位于网站的根目录中，使用特定的语法来指定哪些页面或目录可以被

爬虫访问，哪些则应被禁止。通过合理配置 `robots.txt`，网站管理员可以控制搜索引擎的行为，以保护隐私、避免重复内容索引或管理服务器负载。

40. rust

Rust 是一种系统编程语言，设计目标是提供内存安全和高性能。它采用所有权模型来避免内存错误，同时支持并发编程。Rust 具有现代语法，适合开发系统软件、网络应用和嵌入式系统，受到开发者的广泛欢迎。

41. SGX

SGX（Software Guard Extensions）是英特尔推出的一项安全技术，旨在提供硬件级别的安全性。它允许开发者在受信任的环境中运行代码和处理数据，保护敏感信息不被未授权访问。SGX 创建受保护的执行环境（称为“enclave”），即使在操作系统或其他应用程序被攻破的情况下，数据和代码仍能保持安全。该技术适用于需要高安全性的应用，如金融服务、医疗保健和云计算，确保数据隐私和可信计算。通过 SGX，开发者可以在不可信的环境中安全地执行敏感操作，从而提高应用程序和数据的安全性。

42. 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，以绕过防火墙和地域限制。它通过使用加密来保护用户的隐私，并且可以在各种平台上使用，包括Windows、macOS、Linux、Android和iOS。

ShadowsocksR(SSR)是一个基于Shadowsocks的开源项目，它在Shadowsocks的基础上添加了更多功能和优化。SSR 使用更高级的加密方式，并且支持更多的协议。

43. Shellcode

Shellcode 是一段小的机器代码，用于利用软件漏洞执行攻击者的命令。它通常嵌入在攻击载荷中，通过漏洞注入到程序中。一旦执行，shellcode 可以打开命令行、下载恶意软件或提升权限等。由于其体积小，攻击者会精心设计以避免被检测。了解 shellcode 有助于提高系统安全性。

44. socat

`socat` 是一个多功能的网络工具，用于在两种数据流之间建立双向连接。它可以转发 TCP/UDP 流量、创建代理，并在不同类型的网络协议之间进行桥接。由于其灵活性，`socat` 常用于网络调试、数据转发和安全通信等场景，非常适合网络管理员和开发者。

45. sql注入

SQL 注入是一种攻击技术，攻击者通过在输入字段中插入恶意 SQL 代码，来

操控数据库查询。这种漏洞通常出现在未对用户输入进行充分验证和清理的应用程序中。成功的 SQL 注入攻击可以让攻击者访问、修改或删除数据库中的敏感数据，甚至获取系统的控制权。为了防止 SQL 注入，开发者应该使用参数化查询和预编译语句，并加强对输入的验证和过滤。

46. ssh -D

`ssh -D` 是 SSH 命令的一个选项，用于创建一个 SOCKS 代理。通过这个命令，用户可以将本地端口设置为 SOCKS 代理，允许通过 SSH 隧道转发流量。

```
ssh -D [本地端口] [用户名]@[远程主机]
```

47. ssh -L

`ssh -L` 是 SSH 命令的一个选项，用于创建本地端口转发。通过这个命令，用户可以将本地计算机的端口转发到远程主机的指定端口。

```
ssh -L [本地端口]:[远程主机]:[远程端口] [用户名]@[SSH服务器]
```

48. ssh -R

`ssh -R` 是 SSH 命令的一个选项，用于创建远程端口转发。通过这个命令，用户可以将远程主机的端口转发到本地计算机的指定端口。

```
ssh -R [远程端口]:[本地主机]:[本地端口] [用户名]@[SSH服务器]
```

49. SSO

单点登录（SSO，Single Sign-On）是一种用户身份验证过程，允许用户通过一次登录即可访问多个应用程序或服务，而不需要为每个应用单独登录。SSO 提高了用户体验，减少了记忆多个密码的负担，同时也简化了身份管理。

50. SYN flood

SYN Flood 是一种常见的拒绝服务（DoS）攻击，目的是通过耗尽目标服务器的资源来使其无法处理合法的请求。

工作原理：
TCP 三次握手：正常的 TCP 连接建立需要三次握手过程。客户端发送一个 SYN 包，服务器回应一个 SYN-ACK 包，最后客户端再发送一个 ACK 包。
攻击方式：在 SYN Flood 攻击中，攻击者发送大量伪造的 SYN 包到目标服务

器，但不完成握手过程（不发送 ACK）。这样，服务器会为每个 SYN 请求分配资源，等待确认。
资源耗尽：随着大量未完成的连接请求，目标服务器的连接队列会被填满，最终导致合法用户无法建立连接。
预防措施：
SYN Cookies：通过加密技术在 SYN 包中嵌入信息，服务器无需为每个连接分配资源，直到收到 ACK。
限制连接数：设置连接请求的最大数量，限制来自单个 IP 的连接。
防火墙和入侵检测系统：监控流量并阻止可疑的 SYN 包。
SYN Flood 攻击可以严重影响网络服务的可用性，因此了解并采取防护措施非常重要。

51. tcpdump

`tcpdump` 是一个强大的命令行网络数据包分析工具，用于捕获和分析网络流量。它广泛用于网络故障排除、监控网络活动和安全分析。

52. TOR

TOR（The Onion Router）是一个用于实现匿名通信的网络协议和软件，旨在保护用户的隐私和安全。TOR 通过层层加密和分布式网络结构，使得用户的网络活动难以被追踪。

53. VNC

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进行远程操作。

在网络攻防中，VNC 可能被黑客用来进行远程控制和攻击，因此使用 VNC 时应该配置安全性高的密码，并且应该及时地更新软件。

54. vulhub

Vulhub 是一个开源的项目，旨在为安全研究人员和开发者提供一个方便的环境，用于学习、测试和研究各种网络应用程序的漏洞。它通过 Docker 容器化的方式，提供了多个易受攻击的服务和应用，用户可以在本地或实验环境中进行安全测试。

55. wget

`wget` 是一个用于从网络上下载文件的命令行工具，支持 HTTP、HTTPS 和 FTP 协议。它非常强大且灵活，适合在 Linux 和类 Unix 系统中使用。

56. whois

whois（读作“Who is”，非缩写）是用来查询域名的IP以及所有者等信息的传输协议。简单说，whois就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。我们可以通过whois来实现对域名信息的查询。

早期的whois查询多以命令列接口存在，但是现在出现了一些网页接口简化的线上查询工具，可以一次向不同的数据库查询。网页接口的查询工具仍然依赖whois协议向服务器发送查询请求，命令列接口的工具仍然被系统管理员广泛使用。whois通常使用TCP协议43端口。每个域名/IP的whois信息由对应的管理机构保存。

57. Windows更新服务

Windows 更新服务（Windows Update Service）是 Microsoft 提供的一项功能，旨在自动下载和安装操作系统和应用程序的更新。它可以帮助用户保持系统安全、稳定和最新。

58. Wireshark

Wireshark 是一个强大的开源网络协议分析工具，广泛用于网络故障排除、分析和开发。它能够捕获和以图形化方式展示网络流量，帮助用户理解网络数据包的内容和结构。

59. WriteProcessMemory()

`WriteProcessMemory()` 是 Windows API 中的一个函数，允许一个进程向另一个进程的内存空间写入数据。这个函数通常用于调试、注入代码或修改其他进程的内存。

60. 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。

61. XKMS

XKMS（XML Key Management System）是一种基于 XML 的协议，用于简化

公钥基础设施（PKI）中的密钥管理。它允许用户和应用程序请求和验证公钥的状态和有效性，旨在提高密钥管理的效率和安全性。

62. XSS

XSS（Cross-Site Scripting）是一种常见的网络安全漏洞，攻击者可以利用该漏洞在用户的浏览器中注入恶意脚本，从而窃取用户信息、劫持会话或进行其他恶意活动。

- **存储型 XSS**：
  - 恶意脚本被永久存储在目标服务器上（如数据库），当用户请求该数据时，脚本会被执行。
- **反射型 XSS**：
  - 恶意脚本作为请求的一部分被即时反射回用户的浏览器，通常通过链接或表单提交。
- **DOM 型 XSS**：
  - 攻击者通过修改网页的 DOM 结构来执行恶意脚本，而不需要直接与服务器交互