1. **网络攻防的基本概念** 1.1 **网络安全的属性** **网络空间安全**(Cybersecurity)： 研究网络空间中的安全威胁和防护问题。包括网络空间基础设施的安全和可信，以及网络空间信息的保密性、完整性、可用性、真实性和可控性的相关理论与技术。 **核心属性**（CIA）： **保密性**(Confidentiality)：确保隐私或者秘密信息不向非授权者泄漏，也不被非授权者使用，即：防止数据的未授权访问。 **完整性**（Integrity）：确保信息只能以特定和授权的方式进行改变，比如：确保接收者收到的消息就是发送者发送的消息。 **数据完整性**：确保信息和程序仅以授权方式进行变动 **系统完整性**：确保系统以非损害方式完成设计的功能，免受有意或者无意对系统的非授权操作。 **可用性**（Availability）：合法用户在需要使用网络资源的时候，能够获得正常的服务。 **可控性**：限制对网络资源（软件和硬件）和数据（存储和通信的数据）的访问，其目标是防止未授权使用资源、未授权公开或者修改数据。通过访问控制实现。 **不可否认性**（Non-reputation）：通信实体不能对自己做过的事情抵赖，包括两层含义，一方面发送者不能否认自己发送数据的行为；另一方面，接收者不能否认自己接收过数据。 **真实性**（authenticity）：一个实体是其所声称实体的这种特性。 **可靠性**（reliability）：与预期行为和结果一致的特性。 1.2 **典型网络安全事件：** **Morris worm（蠕虫）、Mirai botnet（DDos）、Stuxnet（震网蠕虫病毒）、WannaCry Ransomware（勒索病毒）、FireEye Redteam tools（泄露事件）、 Solarwinds（供应链攻击事件）** **病毒、蠕虫、木马：**病毒、蠕虫和木马是可导致计算机和计算机上的信息损坏的恶意程序。这三种东西都是人为编制出的恶意代码，都会对用户造成危害。 **计算机病毒**(Computer Virus)，根据《中华人民共和国计算机信息系统安全保护条例》，病毒的明确定义是“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，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”。病毒往往具有很强的感染性、潜伏性、特定的触发性、破坏性。 **病毒必须满足两个条件：自行执行**：它通常将自己的代码置于另一个程序的执行路径中。**自我复制：**例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染个人计算机也可以感染网络服务器。 **蠕虫(worm)病毒**是一种常见的计算机病毒，它利用网络（网络、电子邮件等）进行复制和传播。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中（通常是经过网络连接）。（典型蠕虫病毒：震网病毒、勒索病毒） **普通病毒与蠕虫病毒的区别**：复制方式上，普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制；传染目标上，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。 **木马(Trojan Horse)，**是指那些表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。（是一种用于远程控制的黑客工具、具有隐蔽性、具有非授权性） **隐蔽性**是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，也难以确定其具体位置。**非授权性**是指一旦控制端与服务端连接后，控制端将窃取到服务端的很多操作权限，如修改文件、修改注册表、控制鼠标、键盘、窃取信息等等。 **木马与病毒的区别**：木马不具传染性，它并不能像病毒那样复制自身，也并不“刻意”地去感染其他文件，它主要通过将自身伪装起来，吸引用户下载执行。木马一般主要以窃取用户相关信息或隐蔽性控制为主要目的，相对病毒而言，可以简单地说，病毒破坏你的信息，而木马窥视你。 **软件漏洞** **网络系统的脆弱性：**指系统的硬件资源、通信资源、软件及信息资源等存在的弱点和缺陷。包括硬件系统的弱点和缺陷、软件系统的弱点和缺陷、网络和通信协议的弱点和缺陷、使用者的弱点 **软件安全漏洞**：一台计算机是由硬件以及软件两个部分组成，最基本的软件就是操作系统。 计算机软件是由计算机程序员开发出来的。不同程序员的编程水平不一样，就会造成软件存在这样或者那样的问题，这些问题可能会造成软件崩溃不能运行，我们称这些问题为**软件缺陷（Bug）** 软件中存在的一些问题可以在某种情况下被利用来对用户造成恶意攻击，如给用户计算机上安装木马病毒，或者直接盗取用户计算机上的秘密信息，等等。这个时候，软件的这些问题就不再只是Bug，而是一个软件安全漏洞，简称**“软件漏洞”** 电脑肉鸡：也就是受别人控制的远程电脑。肉鸡可以是各种系统,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。如果服务器软件存在安全漏洞，攻击者可以发起“主动”进攻，植入木马，将该服务器变为一个任人宰割的“肉鸡” **漏洞产生的原因** 1. 小作坊式的软件开发：质量参差不齐 2. 赶进度带来的弊端：投机取巧或者省工省料的办法来开发软件3. 被轻视的软件安全测试：功能为上，测试为下4. 淡薄的安全思想：缺乏安全开发的意识和经验 5. 不完善的安全维护：不重视安全维护，不重视漏洞修复 **漏洞分类：**一个漏洞从被攻击者发现并利用，到被厂商截获并发布补丁，再到补丁被大多数用户安装导致漏洞失去了利用价值，一般都要经历一个完整的生命周期。按照漏洞生命周 期的阶段进行分类的方法包括三种： **0-day漏洞：**指还处于未公开状态的漏洞。这类漏洞只在攻击者个人或者小范围黑客团体内使用，网络用户和厂商都不知情，因此没有任何防范手段，危害非常大。（0-day漏洞也是当前网络战中的核武器） **1-day漏洞：**原义是指补丁发布在1天内的漏洞，不过通常指发布补丁时间不长的漏洞。由于了解此漏洞并且安装补丁的人还不多，这种漏洞仍然存在一定的危害。 **n-day漏洞/已公开漏洞：**已公开漏洞是指厂商已经发布补丁或修补方法，大多数用户都已打过补丁的漏洞。这类漏洞从技术上因为已经有防范手段，并且大部分用户已经进行了修补，危害比较小。 电脑肉鸡是被别人控制的远程电脑。将大量服务器沦为肉鸡，主要依赖于**软件漏洞、木马**。 **漏洞库：**大量软件漏洞需要一个统一的命名和管理规范，以便开展针对软件漏洞的研究，提升漏洞的检测水平，并为软件使用者和厂商提供有关软件漏洞的确切信息。多个机构和相关国家建立了漏洞数据库，这些数据库分为公开的和某些组织机构私有的不公开数据库。公开的数据库包括CVE、NVD、BugTraq、CNNVD、CNVD等。 通过漏洞信息数据库，可以找到操作系统和应用程序的特定版本所包含的漏洞信息，甚至针对某些漏洞的专家建议、修复办法和专门的补丁程序。极少的漏洞库还提供检测、测试漏洞的POC。POC（proof-of-concepts，为观点提供证据）: 样本验证代码。 目前，许多国家建立了针对漏洞的应急响应机构，例如美国计算机应急反应小组US-CERT，中国的国家互联网应急中心CNCERT/CC。他们是软件漏洞数据的主要提供者或者漏洞库的主要维护者，并且提供了高风险的漏洞警报和专家建议。 **美国国家漏洞数据库NVD**（National Vulnerabilities Database）同时收录三个漏洞数据库的信息，CVE漏洞公告、US-CERT漏洞公告、USCERT安全警告，也自己发布漏洞公告和安全警告，是目前世界上数据量最大，条目最多的漏洞数据库之一。 **（美国）通用漏洞列表 CVE(Common Vulnerabilities andExposures)相当于软件漏洞的一个行业标准。**它**实现了安全漏洞命名机制的规范化和标准化**，为每个漏洞确定了唯一的名称和标准化的描述，为不同漏洞库之间的信息录入及数据交换提供了统一的标识，使不同的漏洞库和安全工具更容易共享数据，成为评价相应入侵检测和漏洞扫描等工具和数据库的基准。 **中国国家信息安全漏洞库CNNVD（**China National Vulnerability Database of Information Security）隶属于中国信息安全测评中心，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家级信息安全漏洞库，为我国信息安全保障提供基础服务。 **国家信息安全漏洞共享平台CNVD**（China National VulnerabilityDatabase）是由CNCERT/CC（国家计算机网络应急技术处理协调中心）联合国内重要信息系统单位、基础电信运营商、网络安全厂商建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。 **其他**：EDB漏洞库、微软安全公告板和微软安全建议、绿盟科技的中文安全漏洞库、启明星辰的中文安全公告库 **术语解释**：YARA：一款VirusTotal开发的用于恶意软件识别和分类的规则匹配工具。；Snort：一款历史悠久的开源网络入侵检测系统。； IOC：失陷指标（Indicator Of Compromise），即攻击者控制被害主机所使用的远程命令及控制服务器的相关情报。IOC往往是域名、IP、URL等，这种IOC可部署于安全设备（如：IPS（入侵防御）、SIEM（安全、信息和事件管理）等）进行检测发现甚至实时阻截。； ClamAV：Linux平台上的开源病毒扫描程序，主要应用于邮件服务器，采用多线程后台操作，可以自动升级病毒库。 **安全威胁与安全攻击** **安全威胁**：威胁是指对安全可能的侵害，这种侵害并不意味着实际发生。正因为这种侵害可能发生，因此需要进行防范。如果这种侵害发生了，则称为攻击，而执行攻击行为的主体则称为攻击者。 威胁的主要类型： 信息泄露 、完整性破坏、服务拒绝、未授权访问 **威胁来源**：内部操作不当、内部管理漏洞、外部安全威胁。 **安全攻击**：任何危及到信息安全的行为（安全攻击往往要利用一个或多个威胁） 安全攻击的类型（IATF定义）：被动攻击、主动攻击、物理临近攻击、内部人员攻击、配装分发攻击。 **被动攻击**：攻击者只是窃听消息，不对消息做任何形式的修改。攻击者的目标是获取传输的信息，以便进行利用。 被动攻击的后果：信息内容泄漏、流量模式泄漏 对策：流量加密、流量混淆 常用软件 Wireshark、 Sniffer Pro、TCP Dump、 Snort 典型被动攻击：国家级监控：“棱镜”计划（PRISM） **主动攻击**：避开或破坏安全部件， 引入恶意代码，破坏数据或系统完整性。 如：假冒某个实体主动发送消息、重放旧消息（re-play）、修改传输中的消息、删除选中的消息、各种MiTM攻击。 对策：增强区域边界保护、基于网络管理交互身份认证的访问控制、受保护远程访问、质量安全管理、自动病毒检测工具、审计和入侵检测。 主动攻击特点--可以检测：由于构成系统的物理通信设施、软件和网络协议等存在各种潜在的弱点，因此主动攻击难以绝对防御，但是可以检测。因此，针对主动攻击，重点在于检测并从破坏中恢复过来。 **物理临近攻击** ：一个未授权的个人近距离物理接触网络、系统或设备，以修改、收集信息或者拒绝对信息的访问。这种接近可以通过秘密进入、公开访问或者两者结合。 对策：配置环境监控体系，提供设备物理安全保护 **内部人员攻击**：由在信息安全处理系统物理边界内的合法人员或者能够直接访问信息安全处理系统的人员发起的攻击。 对策：安全意识和训练；审计和入侵检测；安全策略和增强安全性；关键数据、服务和局域网的特殊的访问控制；加强身份识别与认证能力等。 **配装分发攻击**：硬件或软件在生产与安装过程中，或者在运输过程中，被恶意地修改。 对策：可以通过加强处理配置控制将这类威胁降低到最低。通过使用受控分发，或使用由最终用户检验的签名软件和存取控制可以降低分发威胁。