cjs思考题

▼ 第一章 概论

1. **安全要素有哪些？**

   PPT有

   - 可用性：授权实体有权访问数据
   - 机密性：信息不暴露给未授权实体或进程
   - 完整性：保证数据不被未授权修改
   - 可控性：控制授权范围内的信息流向及操作方式
   - 可审查性：对出现的安全问题提供依据与手段

2. **什么是P2DR、PDRR模型？**

   P2DR

   - 将策略、防护、检测和响应四个要素结合起来，提供了一个全面的框架来处理网络安全问题
   - 参考zwh总结“网安补充笔记”

   PDRR

   - 参考zwh“网安补充笔记”

3. **CVE在对漏洞评分时重点评估哪些方面？**

   - CVE：是通用漏洞披露（Common Vulnerabilities and Exposures）的英文缩写，列出了已公开披露的各种计算机安全缺陷，使用CVSS漏洞评分系统评估漏洞严重性
   - CVE系统通过CVSS对漏洞进行评分，其主要评估体现在：基础度量、时效度量、环境度量

- **基础度量组**反映了一个漏洞的固有特征——它不随着时间和用户环境的变化而变化。它由两组指标组成：可利用指标和影响指标。包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响
- **时间度量组**反映了一个可能随时间而变化的漏洞的特征，但是不跨用户环境。例如，一个易于使用的漏洞利用工具包的出现会增加CVSS分数，而一个官方补丁的创建将会减少它。包括可利用性，补救水平，报告信心。
- **环境度量组**代表了一个与某个特定用户环境相关且独特的漏洞的特征。这些度量标准允许分析人员合并安全控制，这些控制可以减轻任何后果，也可以根据她的业务风险促进或降低一个脆弱系统的重要性。1包括攻击向量，攻击复杂性，所需权限，用户交互，范围，机密性影响，完整性影响，可用性影响，机密性要求，完整性要求，可用性要求。

  通过这些度量，CVSS提供了一个全面的、标准化的方法来评估和比较不同漏洞的严重程度。CVSS评分系统可以帮助组织确定漏洞的优先级，从而采取适当的补救措施

4. **为什么看上去大公司会出现更多信息泄露事件？**

- **数据量庞大：**大公司通常处理和存储大量的数据，包括客户信息、财务数据、知识产权和其他敏感信息。数据量越大，潜在的泄露风险就越高。攻击者更有动机针对大公司，因为成功攻击可能带来更大的回报。
- **复杂IT基础设施：**大公司的IT基础设施通常非常复杂，包括多种系统、应用和网络。这种复杂性增加了管理和保护的难度，更容易出现漏洞。旧系统和新系统的整合过程中可能会产生安全漏洞，给攻击者提供了更多的攻击面。
- **更高的曝光率：**大公司在公众和媒体面前曝光率更高。一旦发生信息泄露事件，更容易被报道和放大。相比之下，小公司的信息泄露事件可能不会引起广泛关注，即使发生了也可能被忽视。
- **更有吸引力的目标：**大公司通常拥有更有价值的数据，攻击者会认为对这些公司进行攻击的潜在回报更高。无论是金融数据、知识产权还是客户数据，大公司的数据对攻击者来说往往更有吸引力。
- **内部人员风险：**大公司拥有大量员工，包括全职、合同工和临时员工。更多的人访问和处理敏感数据，增加了内部人员导致信息泄露的风险。这些泄露可能是无意的（如操作失误）或故意的（如内部人员恶意行为）。

- **供应链和第三方风险：**大公司通常依赖于复杂的供应链和众多第三方服务提供商。这些第三方服务可能成为攻击的薄弱环节，攻击者可以通过入侵第三方供应商的系统来间接攻击大公司。
- **安全管理和执行的挑战：**尽管大公司通常有更多的资源投入到信息安全上，但由于其规模庞大，安全政策和措施的执行和管理可能面临更大的挑战。确保所有部门和分支机构都遵守统一的安全标准和实践是复杂的任务。

5. **从棱镜门事件，分析一下美国公共信息安全保障策略的特色**
   - **棱镜门事件：**棱镜门事件（PRISM）是2013年由爱德华·斯诺登曝光的美国国家安全局（NSA）大规模监控项目，通过与微软、谷歌、苹果等大型科技公司的合作，NSA收集了大量互联网用户的数据，包括邮件、聊天记录和文件传输等。此事件揭示了美国政府在全球范围内的广泛监控活动，引发了关于隐私权和政府权力的广泛争议和讨论，并促使美国及国际社会对信息安全和隐私保护进行重新审视和调整。
   - GPT美国公共信息安全保障策略特色：
     - **大规模监控和数据收集：**棱镜门事件表明，美国公共信息安全策略的一个显著特点是大规模监控和数据收集。通过PRISM项目，NSA从多家大型互联网公司获取大量的用户数据，包括邮件、聊天记录、文件存储等。这种策略旨在通过海量数据分析来识别和防止潜在的安全威胁
     - **广泛的国际监控：**棱镜门事件不仅揭示了对美国公民的监控，还显示了对国际目标的广泛监控。美国通过监控全球互联网通信来获取情报，这反映了其信息安全策略的全球视野和对国际事务的深度参与。
     - **与私营企业合作：**美国信息安全策略的另一个重要特点是与私营企业的合作。PRISM项目依赖于与主要科技公司的合作，这些公司包括微软、谷歌、苹果等。政府和私营企业之间的这种合作关系显示了美国在信息安全方面的资源整合和动员能力。
     - **强大的技术支持和资源支持：**美国的信息安全策略得益于强大的技术和资源支持。NSA等情报机构拥有先进的技术能力和丰富的资源，可以执行复杂的大规模数据分析和监控任务。这种技术优势使美国能够在信息安全领域保持领先地位。
     - **法律和政策框架的支持：**棱镜门事件揭示了美国有一套复杂的法律和政策框架来支持信息监控和安全工作。例如，《爱国者法案》（Patriot Act）

和《外国情报监控法》（FISA）为情报机构提供了法律依据和操作规范。这些法律框架使得监控活动在一定程度上合法化，尽管也引发了广泛的隐私和人权争议

- **高度保密和有限的公众知情权：**棱镜门事件还揭示了美国信息安全策略中的高度保密性。很多监控项目在公众和大部分政府官员中都是保密的，只有少数知情者了解其运作细节。这种策略反映了信息安全工作中的隐蔽性和对信息泄露风险的高度防范

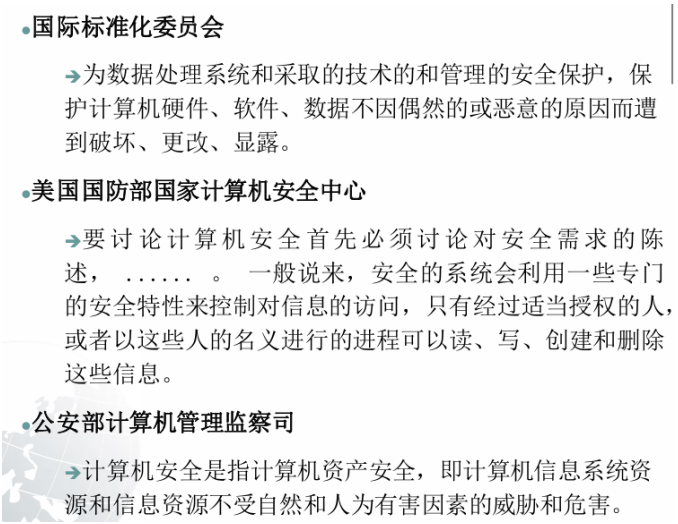
- 安全内参：《“棱镜”十年：美国强化网空情报获取能力活动及其策略分析》
  - **法律授权，披上合法外衣**

> 通过法律给情报行动赋权是美国一贯的做法。2015 年，美国参议院通过《网络安全信息共享法案》，允许私营企业将其用户信息与国土安全部（DHS）共享，要求 DHS 有义务将得到的数据分享给包括 FBI 和 NSA 在内的所有相关政府机构。尽管苹果、谷歌、推特等企业公开表明反对该法案，但是后来不断被曝光的事实显示，这些互联网巨头向美国政府提供了用户数据。
>
> 1978 年，美国颁布《涉外情报监控法》，引入司法审查机制，防止政府部门滥用情报监控权。但是，2001 年“9·11”事件后，美国会先后颁布《爱国者法案》《保护美国法》《涉外情报监控法修正案》，于 2008 年增加第 702 条为正式条款，对《涉外情报监控法》进行修订，允许美情报机构在不经法庭授权的情况下，在美本土监控境外外籍人士的电话和电子邮件。该条款有效期需经过美国国会定期授权，2018 年授权的期限将于 2023 年 12 月 31 日到期。
>
> 702 条款是美情报机构滥用监控特权的“尚方宝剑”。据《纽约时报》报道，2021 年，法院只签发了 300 份秘密搜集美国境内美国人或外国人数据的授权。同年，在 702 条款的框架下，NSA 对境外超过 23 万名外国人进行了电子监控。拜登政府 2023 年 4 月表示，702 条款是美国的“宝贵工具”，帮助美军方、情报机构和执法机关“应对外国威胁”，延长 702 条款有效期是该政府的“关键优先事项”。
>
> 自 1978 年起，美国国会一般每个财年都要通过一部情报授权法，授权该年度情报界计划实施的各类国家情报项目，审批、指导一些重大事项。2016 年 9 月，美国众议院情报委员会向国会提交“针对斯诺登未经授权披露信息的审查报告”，评估斯诺登事件损失、影响及处置效果，指出“NSA尚未有效实施斯诺登事件后的安全改进”，而委员会已在 2014、2015、2016 和 2017 财年《情报授权法案》中采取措施改善情报界信息安全性。

  - **公私合作，强占情报资源：**涉及 9 家美国 IT 巨头公司。在近年来曝出的监听监控事件中，也不乏美国高科技公司的身影
  - **资金保障，确保绝对优势：**美情报机构为了保障情报获取能力不惜重金。“斯诺登事件”曝光的“棱镜”计划每年运营成本为 2000 万美元，相对其后曝出的行动预算“相形见绌”：“奔牛”计划 2013 年运作成本为 2.549 亿美元；2013 年，NSA 向所有合作的电信公司支付了 2.78 亿美元。

6. 你最欣赏哪一种对“安全”的定义？为什么？

请看PPT给的三种安全定义



在对“安全”的定义中，我最欣赏的是国际标准化委员会（ISO）的定义。以下是该定义以及我选择它的原因：

国际标准化委员会的定义

> 安全是为数据处理系统和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。

选择这一定义的原因

1. **全面性**：ISO的定义涵盖了硬件、软件和数据三个关键方面，强调了信息系统的整体保护。这种全面性反映了现代信息安全的复杂性，考虑到了各个可能受到威胁的层面。

2. **综合性保护措施**：定义中提到了技术和管理的安全保护措施，突出了安全不仅仅是技术问题，还涉及管理和策略。这种综合性的视角有助于理解和实施全面的安全策略。

3. **考虑多种威胁**：定义明确指出了对偶然和恶意威胁的防护。这意味着安全措施需要应对广泛的威胁，从意外事故到有针对性的攻击，确保系统的全面防护。

4. **明确的目标**：保护计算机硬件、软件和数据不受破坏、更改和显露，清晰地指出了安全的具体目标。这种明确性有助于制定和评估安全措施的有效性。

其他定义的简评

1. **美国国防部国家计算机安全中心**：
    - 强调了对安全需求的陈述和访问控制，侧重于授权和信息访问控制。这一定义在军事和高度机密环境中非常重要，但可能过于狭窄，未能全面涵盖管理和技术措施。
2. **公安部计算机管理监察司**：
    - 强调了计算机资产的安全，主要关注信息资源和计算机资源的安全性。该定义简洁明确，但在技术和管理措施的细节上不如ISO定义全面。

▼ 第二章 攻击行径分析

1. **哪些社工手段可以被用来获取对网络攻击有价值的信息？**

   \参考zwh的，有

2. **如何搜集整理攻击的相关工具？**

   \参考zwh，这里再扩充一下

   - **确定需求和范围：**明确你需要搜集哪些类型的攻击工具以及这些工具的应用场景。例如，你是关注网络攻击、恶意软件分析还是物理安全漏洞？
   - **利用公开资源：**

A. 安全论坛和社区

- **Reddit**：如r/netsec、r/hacking等板块。
- **Stack Exchange**：如Information Security Stack Exchange。
- **Black Hat**和**Defcon**等安全会议发布的论文和演讲。

B. 安全博客和网站

- **Krebs on Security**：Brian Krebs的博客。
- **Schneier on Security**：Bruce Schneier的博客。
- **The Hacker News**：安全新闻和分析。

C. 开源平台

- **GitHub**：搜索安全工具的代码库，如Metasploit、Nmap、Wireshark等。
- **GitLab**：类似于GitHub的平台。

   - **专业数据库和资源库：**

A. 常见漏洞数据库（CVE）

- **NVD（National Vulnerability Database）**：美国国家漏洞数据库，提供详细的漏洞信息。
- **Mitre ATT&CK**：描述攻击战术和技术的知识库。

B. 安全工具资源库

- **Exploit Database**：包含大量公开的漏洞利用代码。
- **Kali Linux**：提供预装的安全工具，可以用作工具测试和使用的操作系统。

- **订阅安全报告和新闻简报：**
  - **CERT（Computer Emergency Response Team）**：发布关于新威胁和攻击的报告
  - **SANS Internet Storm Center**：提供最新的威胁情报和分析
- **使用安全工具集：**利用专业的安全工具集进行扫描和测试，如Metasploit、Nmap、Wireshark

3. **网络攻击行为经常会留下哪些痕迹？**

   \参考zwh，这里再扩充下

   - **日志文件**
     - **系统日志**：操作系统和应用程序日志中记录的异常活动，如失败的登录尝试、权限提升、系统重启等
     - **网络日志**：网络设备（如路由器、交换机、防火墙）的日志，记录流量模式、连接请求和通信异常。
     - **应用日志**：特定应用程序（如Web服务器、数据库服务器）的日志，记录错误、访问和使用情况。
   - **网络流量分析**
     - **不寻常的流量模式**：如突然增加的网络流量、特定时间段的流量高峰、异常的端口扫描活动
     - **恶意软件通信**：与已知恶意IP地址或域名的通信，或者不明来源的外部连接。
     - **流量异常**：如数据包大小、协议使用和会话持续时间异常

- **系统文件变化**
  - **新文件或文件修改**：恶意软件或攻击者可能会在系统中创建或修改文件。
  - **文件属性变化**：文件的元数据（如创建时间、修改时间）异常。
  - **可疑的执行文件**：在系统关键目录中发现不明来源的可执行文件。
- **系统和进程异常**
  - **不明进程**：在系统中运行的不明或未授权进程。
  - **进程行为异常**：合法进程的异常行为，如高CPU使用率、内存泄漏、异常网络连接。
- **安全设备报警**
  - **IDS/IPS警报**：入侵检测系统（IDS）或入侵防御系统（IPS）发出的警报，提示可能的攻击活动。
  - **防火墙阻断日志**：防火墙记录的被阻止的连接尝试。
- **用户行为异常**
  - **账户锁定**：多个失败的登录尝试导致账户被锁定。
  - **权限提升**：用户账户权限异常提升的记录。
  - **多地登录**：同一账户在短时间内从不同地理位置登录。

4. **网络攻击常用的反跟踪手段有哪些？**

   \zwh也有

   - **使用匿名网络**
     - **Tor网络**：通过多层加密和中继节点，隐藏用户的IP地址和通信内容。
     - **I2P**：另一个匿名网络，提供类似Tor的匿名通信功能。
   - **使用代理服务器和VPN**
     - **代理服务器**：通过中间服务器转发请求，隐藏真实IP地址。
     - **VPN（虚拟专用网络）**：加密通信并隐藏用户的真实IP地址，通过VPN服务器转发流量。

- **加密通信**
  - **SSL/TLS**：使用加密协议保护通信内容，防止被拦截和分析。
  - **暗网**：利用特定的浏览器（如Tor浏览器）访问只在暗网上存在的隐藏服务。
- **伪造和变换**
  - **IP地址伪造**：伪造源IP地址，掩盖攻击者的真实位置。
  - **MAC地址欺骗**：更改网络设备的MAC地址，绕过基于MAC地址的访问控制。
- **清除痕迹**
  - **日志清理**：删除或修改被攻击系统的日志文件，隐藏攻击活动。
  - **系统重启**：通过重启系统覆盖和清除内存中的攻击痕迹。
  - **文件擦除**：使用安全删除工具彻底删除恶意文件，防止被恢复。

▼ 第三章 网络侦察技术

1. **哪里可以方便查询DNS, whois之类信息？**
   - 在线工具
     - DNS查询：MXToolBox、DNSstuff、Google Public DNS
     - Whois查询：Whois.net、ICANN WHOIS、Whois Lookup
   - 命令行工具
     - DNS查询：nslookup、dig
     - Whois查询：whois工具包

2. **同样的域名，为什么我ping的ip地址与别人不同？**
   - **负载均衡**：使用DNS负载均衡技术，将同一域名解析到不同的IP地址，以分散流量和提高可靠性。
   - **地理位置**：CDN（内容分发网络）根据用户的地理位置返回不同的IP地址，以提供更快的访问速度。
   - **DNS缓存**：不同的DNS服务器可能有不同的缓存记录，导致解析结果不同。

- **ISP差异**：不同的互联网服务提供商（ISP）可能使用不同的DNS服务器，从而返回不同的解析结果。

3. **连接80端口成功，一定说明是web服务器吗？连不通，就一定没有web服务器吗？**
   - 连接80端口成功：
     - **不一定是Web服务器**：虽然80端口通常用于HTTP服务，但其他应用程序也可能使用80端口。因此，连接成功并不一定表明目标是Web服务器。
   - 连接80端口失败：
     - **不一定没有Web服务器**：
       - **防火墙**：目标服务器的防火墙可能阻止了80端口的访问。
       - **端口变更**：Web服务器可能配置在其他端口（如8080端口）。
       - **服务器负载**：服务器可能处于高负载状态，导致连接失败。

4. **同一台机器上可以同时运行2个抓包软件吗？**

   可以同时运行，但要注意：

   - **网卡争用**：多个抓包软件同时运行时，会争用同一个网卡，可能导致性能问题或丢包。
   - **权限冲突**：部分抓包软件可能需要独占网卡的权限，从而与其他软件产生冲突。
   - **系统资源**：运行多个抓包软件会消耗更多的系统资源，可能影响系统性能。

5. **跳板机对口令文件破解太慢，怎么办？**

   解决方法：

   - **分布式破解**：使用多台机器协同工作，如使用工具John the Ripper的分布式破解功能。

- **GPU加速**：使用支持GPU加速的工具（如Hashcat），利用GPU的并行计算能力加快破解速度。
- **优化字典**：使用更优化的口令字典，减少无效尝试。
- **使用更强的跳板机**：提升跳板机的计算性能，使用更强大的硬件设备。

6. **哪里可以获得常用口令字典？**

   常用口令字典来源：

   - **SecLists**：GitHub: 包含各种类型的字典，包括密码、用户名、URL等。
   - **Weakpass**：weakpass.com: 提供各种常用口令字典下载。
   - **Rockyou.txt**：著名的密码泄露文件，可以在很多安全资源库中找到。
   - **John the Ripper**：John the Ripper Password Cracker: 提供的常用口令字典。
   - **Kali Linux**：预装了多个常用口令字典，可以在`/usr/share/wordlists`目录下找到。

▼ 第四章 拒绝服务攻击

1. **外部用户针对网络连接发动拒绝服务攻击有哪几种模式？请举例说明**
2. **对付分布式拒绝服务攻击的方法有哪些？举例说明**

▼ 第七章 欺骗攻击

1. **请简述DNS的工作原理，并指出在整个DNS解析过程中，可能存在的被欺骗攻击的地方**
2. **假如你的主机正在面临DNS欺骗攻击，你打算采取什么解决策略和方案？**
3. **Web欺骗攻击有哪些具体形式？请简述其原理。**
4. **假如你负责开发、维护和管理某商业网站，面对潜在的Web欺骗攻击，你将采取哪些手段避免你的网站受到攻击？**

▼ 第九章 访问控制技术

1. **简述口令认证技术的认证方法。用哪些方法可以提高口令认证技术的安全性？**
2. **网络的物理隔离技术包含哪几方面？它们各自采用了什么样的技术？**

3. **什么是基于角色的访问控制技术？它与传统的访问控制技术有什么不同？**
4. **简述四种RBAC模型技术。它们各有什么特点？**

▼ 第十章 防火墙技术

1. **防火墙规则的处理方式中，“Reject”与“Drop”的区别是什么？**
2. **使用应用层代理访问外部Web站点时，会出现访问某些经典网站的响应速度较快，而其他站点响应速度较慢，原因何在？**
3. **如果防火墙允许周边网络上的主机访问内部网络上的任何基于TCP协议的服务，而禁止外部网络访问周边网络上的任何基于TCP协议的服务，给出实现的思路？**

▼ 第十一章 入侵检测

好像木有思考题

▼ 第十二章 VPN技术

1. **VPN的组成**
2. **比较PPTP与L2TP**
3. **简述IPSec中AH协议的功能**
4. **简述IPSec中ESP协议的功能**

第四章-第十二章均与lm思考题一样，答案见zwh资料