“网络”“攻击”与“防范”

“攻击” 5步走：

1. **社会工程:**
   通过社会工程手段，攻击者获取特定目标的信息，例如已知的 QQ 号码
   或非特定目标（机会主义者要控制一批机器当僵尸机）通过钓鱼邮件、假冒网站等方式获取非特定目标的信息。这一步的目的是获取初步的攻击入口。
2. **扫描:**
   攻击者使用各种扫描工具和技术，获取目标系统的漏洞信息。这些工具可以扫描开放端口、操作系统版本、已知漏洞等，以便找到可以利用的安全漏洞。

   工具:

   - **端口扫描器**：如 Nmap，扫描目标开放的端口。
   - **Web 扫描器**：如 Burp Suite、OWASP ZAP，扫描 Web 应用漏洞。
   - **流量抓包工具**：如 Wireshark，捕获并分析网络流量。
   - **SQL 扫描器**：如 SQLMap，扫描和利用 SQL 注入漏洞
3. **入侵**
   在找到漏洞后，攻击者利用这些漏洞进行入侵，获取目标系统的控制权。这一步可能涉及使用恶意软件、远程代码执行等技术手段。

   - **Metasploit**：一个强大的渗透测试框架，包含大量漏洞利用模块。
   - **专用漏洞工具**：如 ms08-067.exe，针对特定漏洞的利用工具。
   - **脚本**：可以从互联网下载黑客编写的脚本，实现快速渗透。
4. **拖库或潜伏监控**
   成功入侵后，攻击者可能会拖库（即窃取数据库中的信息），或者在系统中潜伏，进行长期监控，窃取敏感信息。这一步的目的是获取有价值的数据。

   - **账户信息窃取**：获取用户账户和密码。
   - **网站访问记录**：监控和记录目标的访问活动。
   - **数据盗取**：复制并下载目标系统中的敏感数据。
5. **消除痕迹**
   为了避免被发现，攻击者会消除入侵过程中的痕迹，例如删除日志文件、隐藏恶意软件等。这一步的目的是确保攻击行为不被检测到，从而延长攻击的有效时间。

   - **清理日志文件**：删除或篡改系统日志，隐藏入侵记录。

使用代理和 VPN：通过代理服务器和 VPN 隐藏真实 IP 地址。

使用反取证工具：如 BleachBit，用于彻底删除文件和痕迹。

安全与效率的矛盾

在保证安全的同时，效率可能会受到影响。例如，频繁的安全扫描和防护措施可能会占用系统资源，影响性能。因此，需要在安全和效率之间找到平衡。

这些步骤展示了网络攻击的复杂性和多样性。防御这些攻击需要多层次的安全措施，包括教育用户防范社会工程攻击、及时更新系统补丁、使用入侵检测系统等。

“防范”：

1. **不要泄露社工信息**
   避免在社交媒体、论坛或其他公共场合泄露个人信息和敏感数据，以防止社会工程攻击。
   保持隐私设置，慎重对待陌生人的询问，不随意分享个人信息。
2. **打补丁堵漏洞**
   及时更新系统和软件补丁，修复已知漏洞，防止攻击者利用这些漏洞入侵系统。启用自动更新，定期检查和安装安全补丁，使用可信赖的防火墙和杀毒软件。
3. **观察网络流量，识别正常、异常、攻击，以及拖库等行为(snort,mydlp)**
   通过网络流量监控工具（如 Snort 和 MyDLP）识别异常行为和潜在攻击。
   配置和使用入侵检测系统（IDS）和数据泄漏防护（DLP）系统，设定异常流量警报规则。
4. **对流量载荷中可能的泄露进行检查**（ntop一般不关心载荷）

   检查网络流量载荷中的敏感信息，防止数据泄露。
   使用工具如 Squid + SSLBump + ICAP 进行深度包检测（DPI），过滤和监控网络流量中的敏感数据
5. **日常性的工作**
   保持对系统和网络的持续监控，及时发现和应对潜在威胁。

   观察日志：定期检查系统和网络日志，识别异常活动。

   关心技术论坛和安全新闻：关注最新的安全威胁和补丁信息，保持技术更新，了解新兴的攻击手法和防护措施。

   通过这些措施，可以大大增强系统和网络的安全性，防范各种类型的网络攻击

网络”系统

1. **访问控制 (os、app登录等)**
   访问控制是网络安全的重要组成部分，用于限制未授权用户访问系统资源。
   操作系统和应用登录：通过用户名和密码、双因素认证等方式进行身份验证。

   iptables：一个用于 Linux 系统的防火墙工具，可以配置规则来控制网络流量的进出。

   SELinux：一种增强的安全模块，为 Linux 系统提供强制访问控制。

2. **传输加密**
   传输加密用于保护数据在网络传输过程中的安全，防止数据被截获和篡改。

   HTTPS：通过 TLS/SSL 协议加密 HTTP 流量，确保数据传输的机密性和完整性。

   VPN：虚拟专用网络，通过加密隧道保护远程连接的安全。

   SSH：安全外壳协议，用于加密远程登录和命令执行。

3. **掩盖IP来源**
   掩盖 IP 来源是一种隐私保护措施，防止攻击者追踪用户的真实 IP 地址。
   各种proxy和跳转，典型就是vps、tor、i2p

   Proxy：代理服务器，通过代理服务器中转网络请求，隐藏用户的真实 IP。

   VPS：虚拟专用服务器，通过租用服务器进行网络请求，隐藏用户的真实 IP。

   Tor：洋葱路由网络，通过多层中继节点保护用户的匿名性。

   I2P：不可见互联网项目，通过加密隧道实现匿名通信。

4. **对流量进行其他混淆**
   比如使用ping载荷、dns载荷等
   流量混淆是通过改变流量模式来混淆网络流量，使其难以被检测和分析
   Ping 载荷：在 ICMP Ping 包中隐藏数据，实现隐蔽通信。

   DNS 载荷：通过 DNS 请求和响应中隐藏数据，实现隐蔽通信。

5. **其他**

   Botnet：僵尸网络，通过感染大量计算机形成网络，用于分布式拒绝服务攻击（DDoS）等。

   APT：高级持续威胁，通过长期潜伏和精心策划的攻击，窃取敏感信息。

   供应链攻击：通过攻击供应链上的组件或服务，入侵目标系统。

综合运用这些技术和方法，可以有效提升网络系统的安全性，防范各种潜在的威胁

网络攻击的深层技术（脱离脚本小子的低级趣味）

1. **内存安全**:
   内存安全问题是许多漏洞和攻击手段的基础，尤其是缓冲区溢出。攻击者通过精心构造的数据超出缓冲区的边界，从而覆盖内存中的其他数据，这样可以控制程序执行流，执行任意代码（exploit）或注入恶意代码片段（shellcode）。

2. **二进制分析和逆向**
   通过二进制分析和逆向工程，可以深入理解程序的内部运作机制，发现潜在的安全问题。这适用于各种操作系统和平台，包括 Windows、Linux、Android、macOS 和 iOS。工具如 IDA Pro、Ghidra 和 Radare2 常用于这类分析。

3. **外挂技术**
   外挂技术通常基于对目标程序的深入分析，修改程序的二进制代码或内存数据，以实现某种功能。游戏外挂是这种技术的常见应用，通过修改游戏的内存数据来实现作弊效果

4. **网络攻击**
   现代密码算法设计得非常强大，直接破解密文几乎是不可能的。因此，攻击者通常不直接尝试破译密文，而是通过其他手段获取密钥或利用其他漏洞。例如，通过钓鱼攻击或社会工程获取用户密码，或利用密钥管理中的漏洞进行攻击。

安全管理和法规

1. **安全管理**：“bs7799” vs. 国内网络安全技术标准 vs. 企业安全管理制度

   BS 7799：

   - **背景**：BS 7799 是一套信息安全管理体系（ISMS）标准，由英国标准协会（BSI）发布。它已被 ISO/IEC 27001 所取代。
   - **内容**：BS 7799 包括信息安全管理的最佳实践和控制措施，涵盖了信息安全政策、物理和环境安全、访问控制等多个方面。
   - **目标**：帮助组织建立、实施、运行、监视、审查、维护和改进信息安全管理体系。

   国内网络安全技术标准：

   - **背景**：中国发布了多项网络安全技术标准，以确保国家网络安全。
   - **内容**：涵盖网络安全等级保护、密码使用和管理、网络安全应急响应等。
   - **目标**：提高国家和企业的网络安全水平，保护关键信息基础设施和数据安全。

   企业安全管理制度：

   - **背景**：企业根据自身业务和风险管理需求，制定内部安全管理制度。
   - **内容**：包括信息安全政策、数据保护措施、访问控制、员工培训等。
   - **目标**：确保企业信息和数据的安全，防止泄露和滥用。

2. **国内法规**：~网络安全法、~数据安全法、~个人信息保护法
   网络安全法：
   - **背景**：2017 年生效，旨在保护中国的网络安全。
   - **内容**：包括网络安全等级保护制度、关键信息基础设施保护、网络安全应急响应等。
   - **目标**：确保国家网络安全，保护公民、企业和政府的数据和隐私。

   数据安全法：
   - **背景**：2021 年生效，旨在规范数据处理活动。
   - **内容**：包括数据分类分级保护、数据安全应急处置、数据跨境传输等。
   - **目标**：保护国家安全、公共利益和个人权益，促进数据合理利用。

   个人信息保护法：
   - **背景**：2021 年生效，旨在保护个人信息安全。
   - **内容**：包括个人信息收集、使用、存储、传输等方面的规范，明确个人信息主体的权利。
   - **目标**：保护个人信息不被滥用，确保个人隐私和数据安全。

工具(集)众多，典型举例比如：

1. **泄露案和社工库**
   描述：这些数据库包含已泄露的用户信息，例如电子邮件、密码等。攻击者可以利用这些信息进行社会工程攻击或进一步的渗透测试。
   用途：帮助安全研究人员理解和防范社工攻击，也可用于检查是否存在数据泄露。

2. **安全扫描器以及一些ctf常用工具**
   描述：安全扫描器用于检测系统和网络中的漏洞，常见工具如 Nmap、Nessus 和 OpenVAS。CTF（Capture The Flag）工具用于网络安全竞赛中，帮助参赛者解决挑战。
   用途：发现和修复安全漏洞，提高系统的安全性。

3. **metaspolit**
   描述：一个著名的开源渗透测试框架，提供大量的漏洞利用模块，帮助测试系统的安全性。
   用途：进行漏洞利用和安全测试，验证系统的防护能力。

4. **vulhub**
   描述：一个开源的漏洞环境集合，提供了许多基于 Docker 的漏洞环境。
   用途：用于学习和测试各种漏洞，增强安全技能。

5. **ntopng**
   描述：一个开源网络流量监控工具，可以实时分析和报告网络流量。
   用途：监控网络性能，识别异常流量和潜在威胁。

6. **snort**
   描述：一个开源入侵检测和防御系统，能够实时分析网络流量，检测恶意活动。**用途**：保护网络免受攻击，检测并响应入侵行为。

7. **squid-icap-clamav**
   描述：Squid 是一个代理服务器，ICAP 提供内容适配协议，ClamAV 是一个开源防病毒软件。组合使用可以实现对网络流量的检查和过滤。
   用途：实现内容过滤、恶意软件检测和流量管理。

8. **mydlp**
   描述：一个数据泄露防护（DLP）解决方案，用于监控和保护敏感数据。
   用途：防止数据泄露，保护企业和个人的敏感信息。

9. **ollydbg/x64dbg和IDA**
   描述：OllyDbg 和 x64dbg 是调试工具，用于分析和调试二进制代码。IDA（Interactive DisAssembler）是一个逆向工程工具，用于反汇编和分析二进制文件。
   用途：二进制分析、逆向工程和漏洞研究。

增补的网络安全技术与概念

1. DDOS（分布式拒绝服务攻击）

描述：DDOS 攻击通过使用多个计算机和互联网连接，向目标系统发送大量请求，以压垮系统资源，使其无法正常响应合法用户的请求。

- **防护措施**：使用防火墙和入侵检测系统、网络流量分析、CDN 服务等分布式防护手段。

2. ASLR（地址空间布局随机化）

- **描述**：ASLR 是一种安全技术，通过随机化内存地址来防止缓冲区溢出等漏洞被利用。

- **优势**：增加攻击者预测和利用内存地址的难度，提高系统安全性。

3. 撞库

- **描述**：撞库是指攻击者利用用户在不同网站使用相同的用户名和密码的习惯，进行大规模的密码尝试，攻击其他网站账户。

- **防护措施**：建议使用不同网站不同的密码、开启双因素认证、使用密码管理器生成和存储强密码。

4. 安全地分析计算机病毒

描述：安全分析计算机病毒需要使用隔离的沙箱环境，以免病毒扩散和感染其他系统。

工具和技术：

虚拟机和沙箱：使用虚拟机（VMware、VirtualBox）或沙箱（Cuckoo Sandbox）隔离环境进行分析。

静态分析：使用反编译工具（如 IDA Pro）分析病毒代码。

动态分析：在隔离环境中运行病毒，观察其行为和网络活动。

5. 渗透测试

描述：渗透测试是模拟攻击者对系统进行测试，以发现和修复潜在漏洞。

过程：包括信息收集、漏洞扫描、利用漏洞、权限提升和报告撰写。

工具：Metasploit、Nmap、Burp Suite、Nessus 等。

6. 蜜罐（Honeypot）

描述：蜜罐是一种安全资源，用于诱骗和检测攻击者。它模拟真实的系统或服务，但实际上是监视和记录攻击者行为的工具。

类型：高互动蜜罐（High-Interaction）、低互动蜜罐（Low-Interaction）。

用途：监控和分析攻击者的技术和策略，提高网络防御能力。

结课阅读

========

网络攻击(与防范)几步走，学习线索串联如下：

【1】**了解目标，通过社会工程**，比如至少whois一下，利用“社工库”也是重要的手段之一。所以社工库是违法的，不过建设和部署一个用于内部自用教育培训和演示的社工库系统希望***。

【2】**对目标主机或网络进行安全扫描**，注意别暴漏自己，有个叫董大风(化名)的仅扫描了某政府网站一下，就被判了几个月，用的还是境外的VPS，实在不行，“撒旦”了解一下。反过来，防范工作在扫描阶段就开始了，用防火墙、snort等易于发现扫描行为，应及时预警(向上级汇报)，如果是政府网站就可以请律师了。只报警是不行的，要打补丁要改配置要买防火墙，一定要买。

【3】**有了目标的漏洞信息**，可以用通用工具比如Metasploit等尝试获得控制权。如果漏洞太新，比如安全论坛看到的0day，流行工具还没有收录，只能论坛里找别的黑客写好的工具比如MSxx-yyy.exe这种，或自己写利用漏洞入侵的程序(共享给别人利用是违法的)。

【4】**有了控制权，先偷文件**，再长期驻留监控用户活动，也可以当攻击跳板或代理，也可以利用其CPU、存储、带宽等资源做些能获得利益的事情。不要做损人不利己的事情。从防范角度，装终端安全软件如360或Symantec，配置windows安全域(活动目录)，装mydlp等，是能阻止或发现不正常的进程、文件、网络等活动的。

【5】**全身而退 vs. 追踪痕迹。**攻击的敏感步骤，应尽量通过vps、tor、i2p等难于追踪的间接通信形式，要把系统中各种活动日志等及时清空或破坏，选择温和低调的策略以利于长期隐藏等。

【6】**攻、防双方都应了解和熟悉相关的法律**，要阅读“中华人民共和国网络安全法”“中华人民共和国数据安全法”“中华人民共和国个人信息保护法”。不仅是黑客，还有网管也要了解哪些途径自己可能进去。本市某儿童照相馆买、卖公民个人信息，用于电话营销，被公安部列入年度十大典型案件。https://www.mps.gov.cn/n2254098/n4904352/c9148603/content.html

其他知识点：

---

1. 内存安全之缓冲区溢出（BOF）

缓冲区溢出（Buffer Overflow, BOF） 是一种常见的内存安全漏洞。攻击者通过向缓冲区写入超过其容量的数据，覆盖相邻内存区域，从而执行任意代码。

- **漏洞利用**：编写特定的输入数据，覆盖返回地址或函数指针，劫持程序控制流。
- **防护措施**：启用 ASLR、使用堆栈保护（Canaries）、边界检查等。

2. 传输加密技术

传输加密技术 确保数据在网络传输中的机密性和完整性，防止被窃听和篡改。

- **VPN**：虚拟专用网络，通过加密隧道保护远程连接的安全。
- **SSH**：安全外壳协议，用于加密远程登录和命令执行。
- **HTTPS**：通过 TLS/SSL 协议加密 HTTP 流量，确保数据传输的安全性。
- **中间人攻击**：攻击者拦截和篡改通信数据，SSLBump 和 ICAP 可以用于检测和防御这种攻击。

3. 逆向分析技术路线、工具和方法

逆向分析 通过分析可执行文件的内部结构和行为，理解其功能和查找潜在漏洞。

- **技术路线**：二进制文件反汇编、动态调试、静态分析、代码逆向。
- **工具**：IDA Pro、Ghidra、Radare2、OllyDbg、x64dbg 等。
- **方法**：静态分析用于理解代码结构和逻辑，动态分析用于运行时行为观察。

4. 代理和端口映射技术和工具

代理和端口映射技术 用于网络流量的中转和重定向，保护隐私和穿透防火墙。

- **HTTP Proxy**：通过代理服务器中转 HTTP 请求，隐藏用户真实 IP。
- **SOCKS Proxy**：支持多种协议的代理，常用于翻墙和隐私保护。
- **Socat**：一个多功能的网络工具，用于数据流的转发和重定向。
- **SSH 隧道**：使用 SSH 创建安全隧道，实现远程端口转发（-L/-R）和动态端口转发（-D）。

SSR：ShadowsocksR，用于加密和代理流量，突破网络封锁。

答疑之crack7475爆破法

比如有这样一个程序，do()函数需要用户输入正确的key才返回非零，程序才干活，否则直接退出了。

```
main()
{
	if (!do_you_have_key())
		exit(-2);
	// do work
	return 0;
}
```

观察（用比如visual studio）可见C代码对应的汇编代码如下：

```
   22: main()
   23: {
   24:       if (!do_you_have_key())
00401050 E8 AB FF FF FF    call        do_you_have_key (401000h)
00401055 85 C0             test        eax,eax
00401057 75 14             jne         main+1Dh (40106Dh)
   25:       {
```

把“75 14”中的75改成74，就相当于把if语句中的叹号拿掉，效果就是输入一个正确的key反而直接退出了，输入一个错误的可以反倒能干活。

这种方法是常见的软件破解方法，找对了位置，只要修改一个bit就达到目的。

实际实施的时候，可以修改磁盘上exe/dll文件，也可以修改内存中进程代码段中的代码的机器指令字节。
