网络空间安全工程技术人才培养体系指南

（版本2.0）

中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟

二〇一九年十二月

© 2019 中国网络空间安全人才教育联盟

联合发布（2.0 版）

广州大学

南开大学

华中科技大学

湖南会览网安教育服务有限公司

湖南合天智汇信息技术有限公司

版权声明

本指南（2.0 版）版权属于中国网络空间安全人才教育联盟、广州大学、南开大学、华中科技大学、湖南会览网安教育服务有限公司、湖南合天智汇信息技术有限公司共同所有，受法律保护。转载、摘编或利用其他方式使用白皮书文字或者观点，应注明“来源：中国网络空间安全人才教育联盟”，并书面知会联盟秘书处。违反上述声明者，本指南权利者保留追究其法律责任的权利。

免责声明

本指南仅供参考。对于本文档中的信息，联盟及联合发布单位不作明示、默示保证。本指南基于现状编写。在指南中的信息和意见，均可能会改变，不另行通知。您需自行承担使用风险。

词汇说明

文中“网安人才”特指网络空间安全工程技术人才。

第一次印刷：2019 年 12 月 17 日

引 言

网络空间作为人类社会生存和发展的新空间，成为了“陆、海、空、天、网”中的第五维新疆域，党和国家领导人高度重视网络空间安全问题，习近平总书记亲自担任中共中央网络安全和信息化委员会主任，就网络空间安全问题多次作出重要指示。网络空间安全问题进入到国家战略强势介入的全新阶段。

针对我国目前对有实践经历和实战能力的网络空间安全工程技术人才（以下及正文简称“网安人才”）需求缺口巨大、需求增速不断加快的现实，中国网络空间安全人才教育联盟会聚成员单位提出了我国网安人才培养框架，在《网络空间安全工程技术人才培养体系指南》（以下简称“指南”）中对框架的网安人才层次化培养体系、知识技能体系、认证体系等主体部分进行了论述。其中的“知识技能体系”，就从业人员业务标签这一全新角度，参考学科专业体系，梳理提出了网安人才知识技能体系，突出以“人”为核心、以“知识技能”为业务内容，为工程技术人才培养和考核认证提供参考。

“指南”采取迭代补充更新的发布方式，目前已发布的“1.0 版”包括了层次化培养体系、知识技能体系（含 Web 安全、网络渗透、安全运维三个实例）、认证体系。当前发布的“2.0 版”在“1.0 版”基础上，补充更新了“逆向分析”、“漏洞挖掘与利用”、“恶意代码”和“溯源取证”四个实例。“指南”的各个发布版本是一个有机整体，在理论和实施层面均是不可分割的，后续版本是对之前版本的补充更新。

本指南（2.0 版）由中国网络空间安全人才教育联盟联合广州大学、南开大学、华中科技大学、会览网安、合天智汇共同发布。

 ©2019 中国网络空间安全人才教育联盟

本指南（含当前及之前发布版本）编写过程中，参考了国家机关、中国工程院等机构研究发布的人才培养数据和观点，得到了行业专家的帮助指导，在此一并表示感谢。他们是（姓名英文字母序）:

崔　翔（广州大学）

廖　鹏（南瑞集团）

刘宝旭（中科院信工所）

刘潮歌（中科院信工所）

刘建伟（北京航空航天大学）

刘奇旭（中科院信工所）

刘哲理（南开大学）

鲁　辉（广州大学）

田志宏（广州大学）

王　乐（广州大学）

薛继东（丁牛科技）

杨　珉（复旦大学）

杨　卿（360 集团）

邹德清（华中科技大学）

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

目 录

引 言……I

第一章 网安人才培养框架……（参见 1.0 版）

第二章 网安人才层次化培养体系……（参见 1.0 版）

第三章 网安人才知识技能体系……（参见 1.0 版）

3.1 体系分类方法……（参见 1.0 版）

3.2 标签化知识技能体系……（参见 1.0 版）

3.3 体系展开实例……（参见 1.0 版）

1. Web 安全知识技能体系……（参见 1.0 版）

2. 网络渗透知识技能体系……（参见 1.0 版）

3. 安全运维知识技能体系……（参见 1.0 版）

4. 逆向分析知识技能体系……1

（1）逆向分析基础……1

（2）低级语言分析……1

（3）文件格式分析……2

（4）逆向分析工具使用……3

（5）常见算法分析……3

（6）静态分析对抗……3

（7）动态调试对抗……4

（8）脱壳分析……4

5. 漏洞挖掘与利用知识技能体系……4

（1）基础知识……5

（2）二进制插桩……5

（3）符号执行……6

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

（4）漏洞挖掘……6
（5）漏洞利用……6
（6）缓解机制绕过……7
6. 恶意代码知识技能体系……7
（1）自动传播……9
（2）驻留与持久化……9
（3）远程控制与数据回传……9
（4）情报获取……10
（5）降级与破坏……10
（6）规避与对抗……10
7. 溯源取证知识技术体系……11
（1）数据和权限恢复……11
（2）网络欺骗与诱捕反制……12
（3）日志审计……13
（4）用户与设备追踪……13
（5）隐私数据挖掘……13
（6）数据分析与用户画像……14
3.4 知识技能体系的应用……（参见 1.0 版）
第四章 网安人才认证体系……（参见 1.0 版）
附 中国网络空间安全人才教育联盟……15

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

第三章 网安人才知识技能体系

3.3 体系展开实例

在指南的 1.0 版已展开的“1. Web 安全”、“2. 网络渗透”、“3.安全运维”基础上，2.0 版选取逆向分析、漏洞挖掘与利用、恶意代码和溯源取证四个子体系展开描述，并采用思维导图方式简介其三级节点。

4. 逆向分析知识技能体系

逆向分析是网络攻防体系中的一项重要基础技能，不管是恶意代码分析还是漏洞分析，都要求研究者具备良好的逆向分析能力。逆向分析从知识技能视角可划分为逆向分析基础、低级语言分析、文件格式分析、逆向分析工具使用、常见算法分析、静态分析对抗、动态调试对抗、脱壳分析等。

（1）逆向分析基础

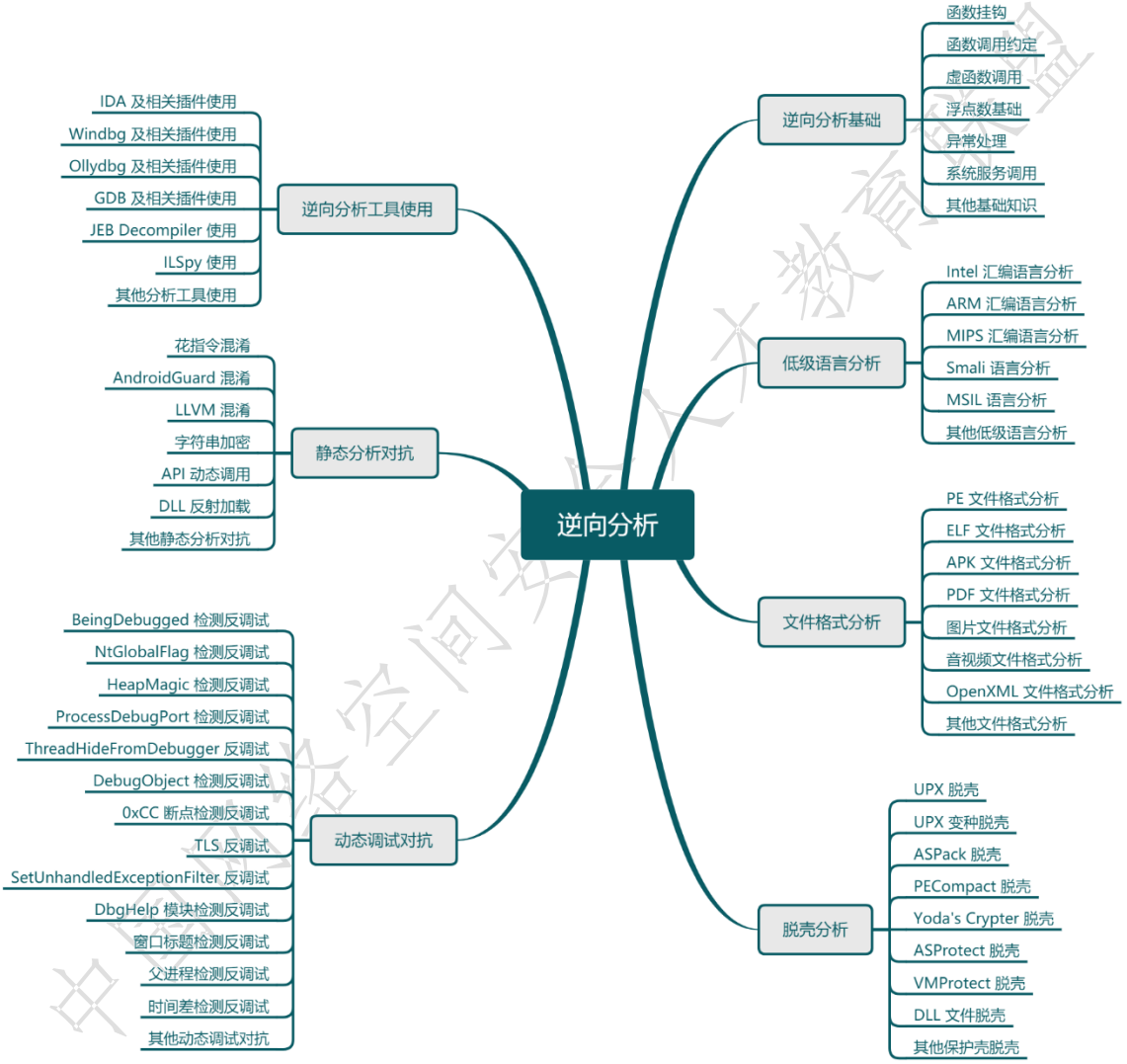
逆向分析基础涵盖了研究者应掌握的理论知识和实践能力，涉及操作系统、网络协议、密码学等理论知识，以及汇编语言、C/C++ 语言、脚本语言等常见编程语言的阅读和编写能力。逆向分析基础主要技术包括函数挂钩、函数调用约定、虚函数调用、浮点数基础、异常处理、系统服务调用等。

（2）低级语言分析

低级语言（Low-level Programming Language）通常指汇编语言。在没有编译器的情况下，其按照标准文档可以与机器指令互相转换，也正因为如此，二进制程序在没有源代码的情况下可以被反汇编成汇编语言，逆向分析通常基于反汇编代码进行分析。与二进制程序

 ©2019 中国网络空间安全人才教育联盟

被反汇编成汇编代码类似，脚本语言代码编译后生成的字节码文件可以被反编译成对应的中间语言，并且中间语言通常可以被还原成类似原始脚本语言源代码的结果。低级语言分析主要技术包括 Intel 汇编语言分析、ARM 汇编语言分析、MIPS 汇编语言分析、Smali 语言分析、MSIL（Microsoft Intermediate Language）语言分析等。



（3）文件格式分析

文件格式（File Format）指文件的内部构成方式。在计算机系统中，文件格式类型多种多样，但对机器本身而言均为二进制数据格式，文件格式只对特定类型的解析器（Parser）而言才有意义，例如

 ©2019 中国网络空间安全人才教育联盟

多媒体播放器可以解析各种音视频文件、字处理程序可以解析各种文档文件、看图软件可以解析各种图片文件等。通常而言，特定类型的文件格式都有一个对应的格式规范，其通常可以从厂商或国际标准化组织获取。文件格式分析是逆向分析的一个重要组成部分，其主要相关技术包括 PE（Portable Executable）文件格式分析、ELF（Executable and Linkable Format）文件格式分析、APK（Android Package）文件格式分析、PDF（Portable Document Format）文件格式分析、图片文件格式分析、音视频文件格式分析、OpenXML 文件格式分析等。

（4）逆向分析工具使用

借助已有的逆向分析工具以及相关插件、或者自己实现相关的分析工具，可以有效减少重复劳动、甚至是极大的提高逆向分析的效率。逆向分析工具主要包括 IDA 及相关插件使用、Windbg 及相关插件使用、Ollydbg 及相关插件使用、GDB 及相关插件使用、JEB Decompiler 使用、ILSpy 使用等。

（5）常见算法分析

一个功能完善的程序在实现过程中经常会使用一种或多种算法，在逆向分析过程中，如果不能快速识别一个程序所使用的算法，那么逆向分析人员很有可能会耗费大量的时间也难以解决问题。有效识别目标程序所使用的算法，则能有效加快逆向分析人员的进度。常见算法分析技术包括 CRC32 算法分析、Base64 算法分析、MD5 算法分析、SHA1 算法分析、RC4 算法分析、AES 算法分析、RSA 算法分析等。

（6）静态分析对抗

逆向对抗（即反逆向）与逆向分析是一场持久的对抗战争。逆

 ©2019 中国网络空间安全人才教育联盟

向分析人员可以通过逆向分析来理解目标程序的内部实现逻辑，开发人员也可以通过相关技术来提升逆向分析人员的分析成本，以降低程序在短时间内被其他人员成功逆向分析的风险。根据逆向分析方式的不同，逆向分析对抗技术可以划分为静态分析对抗与动态调试对抗。静态分析对抗主要技术包括花指令混淆、Android Guard 混淆、LLVM 混淆、字符串加密、API 动态调用、DLL 反射加载等。

（7）动态调试对抗

动态调试对抗即检测当前程序是否正在被调试器调试，如果是则做出相应的对抗行为，例如进入不同的代码分支、退出进程、甚至是利用调试环境的漏洞发起攻击等。动态调试对抗主要技术包括 Being Debugged 检测反调试、NtGlobalFlag 检测反调试、HeapMagic 检测反调试、ProcessDebugPort 检测反调试、ThreadHideFromDebugger 反调试、DebugObject 检测反调试、0xCC 断点检测反调试、TLS（Thread Local Storage）反调试、SetUnhandledExceptionFilter 反调试、DbgHelp 模块检测反调试、窗口标题检测反调试、父进程检测反调试、时间差检测反调试等。

（8）脱壳分析

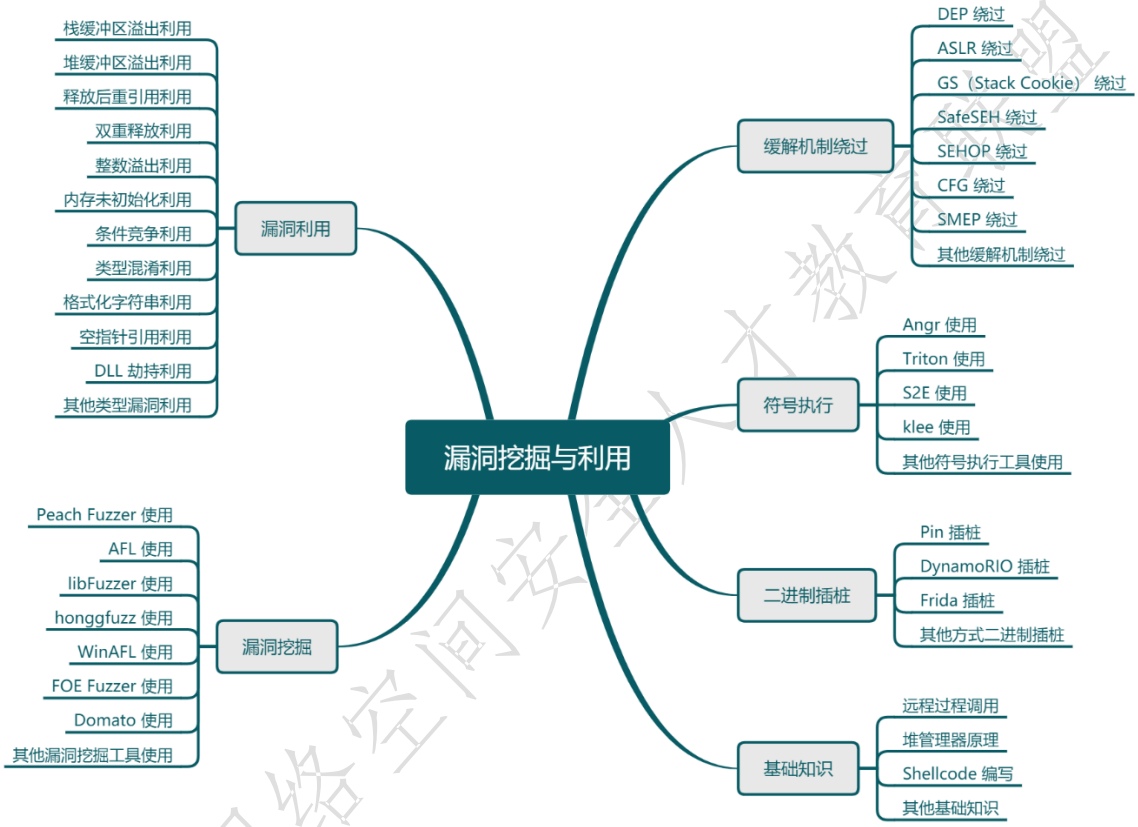
加壳程序可以在不改变原有程序功能的基础上为其提供一层“保护壳”，从而极大的提升逆向分析的成本。对于经过加壳保护的程序，逆向分析人员的首要工作是对其进行脱壳，之后才能进行后续分析工作。脱壳分析主要技术包括 UPX 脱壳、UPX 变种脱壳、ASPack 脱壳、PECompact 脱壳、Yoda’s Crypter 脱壳、ASProtect 脱壳、VMProtect 脱壳、DLL 文件脱壳等。

5. 漏洞挖掘与利用知识技能体系

漏洞挖掘与利用是网络攻防核心组成部分，攻击者借助漏洞可

 ©2019 中国网络空间安全人才教育联盟

以实现远程代码执行、恶意代码投递、权限提升等攻击。漏洞利用方式具有多样性和隐蔽性的特点，受害者点开一个 URL 链接、打开一个文档、甚至是完全不进行任何操作都有可能被攻击者获取系统权限。漏洞挖掘与利用从知识技能视角可划分为基础知识、二进制插桩、符号执行、漏洞挖掘、漏洞利用、缓解机制绕过等。



（1）基础知识

漏洞挖掘与利用基础知识涵盖了研究者在该研究领域中应当掌握的理论知识和实践能力，涉及汇编语言、C/C++ 语言、脚本语言等常见编程语言的阅读和编写能力，以及进程管理、内存管理等操作系统基本原理。漏洞挖掘与利用基础技术包括了逆向分析基础技术、远程过程调用、堆管理器原理、Shellcode 编写等。

（2）二进制插桩

 ©2019 中国网络空间安全人才教育联盟

插桩（Instrumentation）是指向源代码或者二进制程序插入额外的代码，以便监控程序性能、跟踪代码执行路径、以及辅助发现软件漏洞等。插桩可以分为源代码 / 编译器插桩（Source / Compiler Instrumentation）和二进制插桩（Binary Instrumentation），后者又可以细分为静态二进制插桩（Static Binary Instrumentation）和动态二进制插桩（Dynamic Binary Instrumentation）。二进制插桩是辅助漏洞挖掘与利用的一种有效方式，其主要技术包括 Pin 插桩、DynamoRIO 插桩、Frida 插桩等。

（3）符号执行

符号执行（Symbolic Execution）是一种程序分析技术，其通过分析程序得到让特定代码区域执行的输入。使用符号执行分析特定程序时，该程序会使用符号值作为输入，而非一般执行程序时所使用的具体值；在到达目标代码时，分析器可以得到相应的路径约束，然后通过约束求解器来得到可以触发目标代码的具体值。符号执行主要技术包括 Angr 使用、Triton 使用、S2E 使用、Klee 使用等。

（4）漏洞挖掘

漏洞挖掘是指通过人工分析或者自动化的方法来发现程序中存在的漏洞，是漏洞利用的先决条件。模糊测试（Fuzz Testing / Fuzzing）是工业界普遍采用的一种高效的自动化漏洞挖掘方式，其核心思想是自动或半自动的生成随机数据输入到一个程序中，并通过监控程序的异常信息来发现可能存在的错误。漏洞挖掘主要技术包括 Peach Fuzzer 使用、AFL 使用、libFuzzer 使用、honggfuzz 使用、WinAFL 使用、FOE Fuzzer 使用、Domato 使用等。

（5）漏洞利用

漏洞利用（Exploit）是指利用程序中的一个或多个漏洞来实现

 ©2019 中国网络空间安全人才教育联盟

攻击者想要达到的攻击效果，如远程代码执行（Remote Code Execution）、信息泄露（Information Disclosure）、权限提升（Privilege Escalation）等。漏洞利用是漏洞攻防核心能力的体现，经验丰富的安全研究人员通常只需要利用一个漏洞即可达到想要的攻击效果。漏洞利用主要技术包括栈缓冲区溢出（Stack Buffer Overflow）利用、堆缓冲区溢出（Heap Buffer Overflow）利用、释放后重引用（Use After Free）利用、双重释放（Double Free）利用、整数溢出（Integer Overflow）利用、内存未初始化（Uninitialized Memory）利用、条件竞争（Race Condition）利用、类型混淆（Type Confusion）利用、格式化字符串（Format String）利用、空指针引用（Null Pointer Dereference）利用、DLL 劫持（DLL Hijacking）利用等。

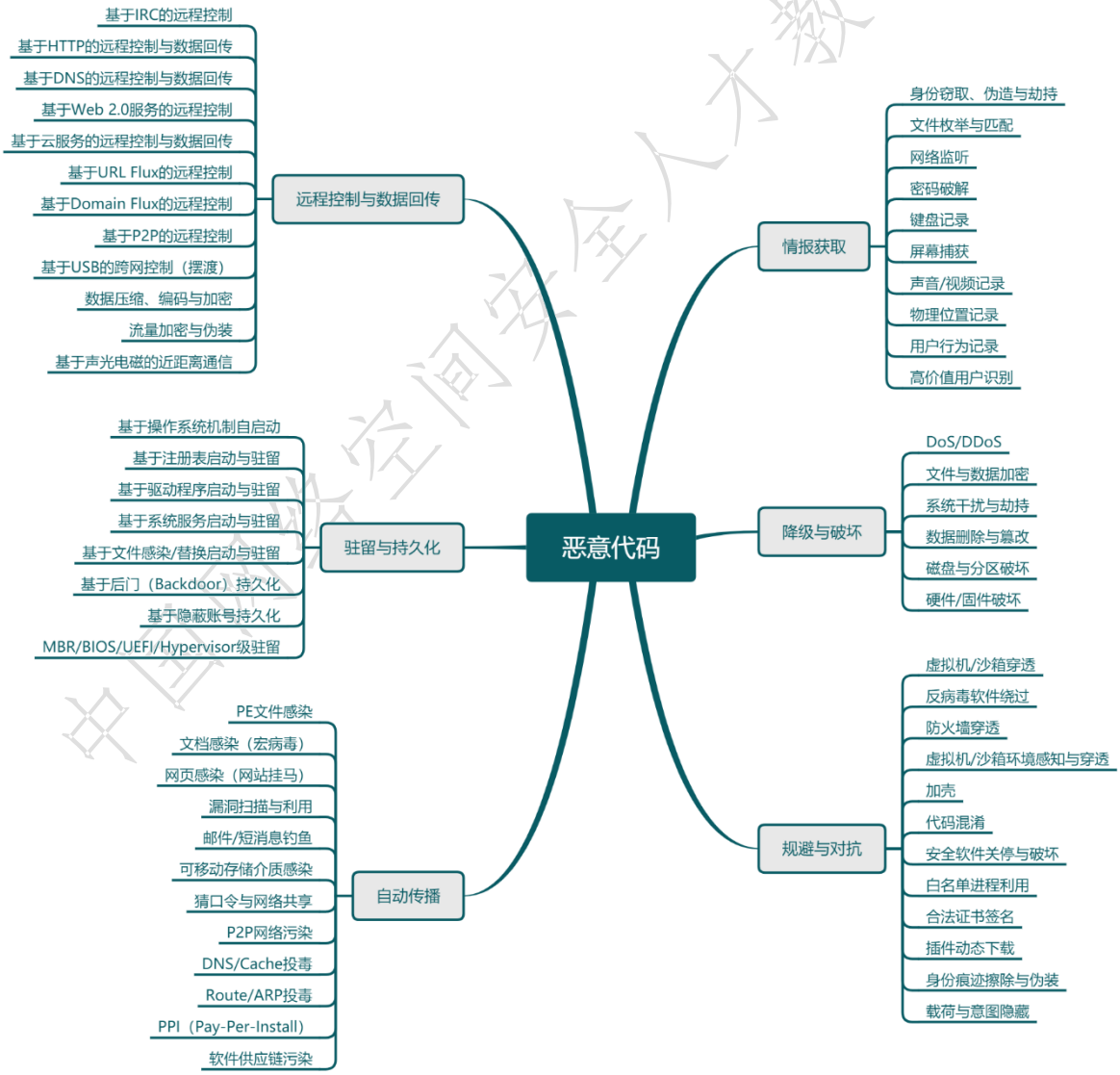
（6）缓解机制绕过

漏洞攻击与防御是一对矛盾对立的统一体，它们相互制约却又共同发展。针对层出不穷的漏洞利用方式，软硬件厂商提出并实现了各种漏洞利用缓解机制，以干扰传统漏洞利用方式的正常使用。然而新的缓解机制并不可能在相当长的时间里保持理想的防御效果，因为攻击者往往也能想出对应的缓解机制绕过技术。为了实现更好的漏洞利用缓解机制，软硬件厂商甚至会重金悬赏未知的缓解机制绕过技术，如微软的 Mitigation Bypass 奖励计划。缓解机制绕过主要技术包括 DEP 绕过（Data Execution Prevention Bypass）、ASLR 绕过（Address Space Layout Randomization Bypass）、SafeSEH 绕过（SafeSEH Bypass）、SEHOP 绕过（SEH Overwrite Protection Bypass）、CFG 绕过（Control Flow Guard Bypass）、SMEP 绕过（Supervisor Mode Execution Prevention Bypass）等。

6. 恶意代码知识技能体系

 ©2019 中国网络空间安全人才教育联盟

恶意代码是网络攻防核心组成部分，近年曝光的绝大多数重大网络安全事件，都与恶意代码紧密相关。恶意代码从表现形态视角可分为释放器（Dropper）、下载器（Downloader）、键盘记录器（Keylogger）、逻辑炸弹（Logic Bomb）、后门（Backdoor）、病毒（Virus）、蠕虫（Worm）、木马（Remote Access Trojan）、僵尸程序（Bot）、间谍软件（Spyware）、勒索软件（Ransomware）、挖矿劫持（Cryptojacking）软件等；从知识技能视角则可划分为自动传播、驻留与持久化、远程控制与数据回传、情报获取、降级与破坏、规避与对抗。



中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

（1）自动传播

定向渗透具有人工干预多、目标确定的特性，相比而言，自动传播则具有人工干预少、目标群体大且随机性强的特性。自动传播技术赋予恶意代码自我复制和持续再生的能力，堪称恶意代码区别于其他网络攻击形态的独有特性。自动传播主要技术包括 PE（Portable Executable）文件感染、Office 文档感染（宏病毒）、漏洞扫描与利用、可移动存贮介质感染、网页感染（网站挂马）、猜口令与网络共享、P2P 网络污染、软件供应链污染等。

（2）驻留与持久化

绝大多数恶意代码一旦传播到目标系统上并获得代码执行机会，首先要解决的问题就是系统重启后如何让自身再次获得执行机会而又不引起明显异常，从而实现尽可能长时间的生存。当然，也有极少量的恶意代码仅存在于内存之中，断电或重启则会消失。这类恶意代码（如红色代码蠕虫）或者依托快速自动传播能力实现总体规模平衡，或者一次性运行即可完成任务。驻留与持久化主要技术包括基于注册表启动与驻留、基于系统服务启动与驻留、基于文件感染启动与驻留、MBR/BIOS/UEFI/Hypervisor 级驻留、基于隐蔽账号持久化、基于后门（Backdoor）持久化等。

（3）远程控制与数据回传

远程控制从根本上改变了传统病毒和蠕虫攻击成果无法再利用的局面，堪称是一种“不会过时”的攻击技术。远程控制主要是针对僵尸网络（Botnet）、远控木马（Remote Access Trojan，RAT）而言的，僵尸网络侧重建立健壮的命令与控制信道（Command and Control Channel）来管理大规模“瘦客户”，而远控木马侧重建立轻量级命令与控制信道管理小规模“胖客户”。此外，严格来说，对大规模后门的安全访问，也应列入远程控制范畴。数据回传，指的是将

 ©2019 中国网络空间安全人才教育联盟

被控端上的感兴趣数据以良好的穿透性、隐蔽性回传给攻击者的过程。远程控制与数据回传主要技术包括基于 Domain Flux/URL Flux 的动态远程控制、基于应用层协议的远程控制与数据回传、基于 USB 的跨网控制、基于声光电磁的近距离通信、流量加密与伪装等。

（4）情报获取

获取情报是恶意代码主要危害之一。远控木马和僵尸程序常常窃取用户身份信息以获取经济利益，而 APT 中的恶意代码更关注敏感文件、键盘与屏幕等可获取商业与军事机密的情报，可以说获取情报是当前绝大多数 APT 的首要任务。获取情报后，一般需要加密、压缩、编码后回传给攻击者，并防止通信链路上被监听、检测和破译。情报获取主要技术包括身份窃取、键盘记录、屏幕捕获、声音/视频记录、文件枚举与匹配、高价值用户识别、物理位置记录等。

（5）降级与破坏

对信息系统造成降级和破坏是恶意代码的主要危害之一。2005 前的蠕虫曾经造成互联网多次拥塞；僵尸网络一直都是发起分布式拒绝服务攻击（DDoS）的最主要依托平台；2013 年开始流行的勒索软件可对文件、数据库和硬盘进行加密劫持；2018 年盛行的挖矿劫持（Cryptojacking）软件可耗费国家电力能源和用户计算资源；APT 攻击可破坏重要设备或干扰重要信息系统正常运行。降级与破坏主要技术包括拒绝服务、文件与数据加密、系统干扰与劫持、硬件/固件破坏等。

（6）规避与对抗

从 DOS 时代起，病毒与杀毒软件的对抗就已拉开帷幕并不断升级演进。今天的恶意代码采用的规避手段早已超越病毒时代的 EPO、多态、变形和加壳，而且已不限于纯技术手段，而杀毒软件也从单

 ©2019 中国网络空间安全人才教育联盟

一化终端软件演化为端-网-云全覆盖、融入人工智能技术、具备态势感知能力的叠加演进防御体系。主机层面的恶意代码采用的规避与对抗技术主要包括反病毒软件绕过、虚拟机/沙箱识别与穿透、防火墙穿透、代码混淆、安全软件关停与破坏、合法证书签名、插件动态下载、身份痕迹擦除与伪装、载荷与意图隐藏等。

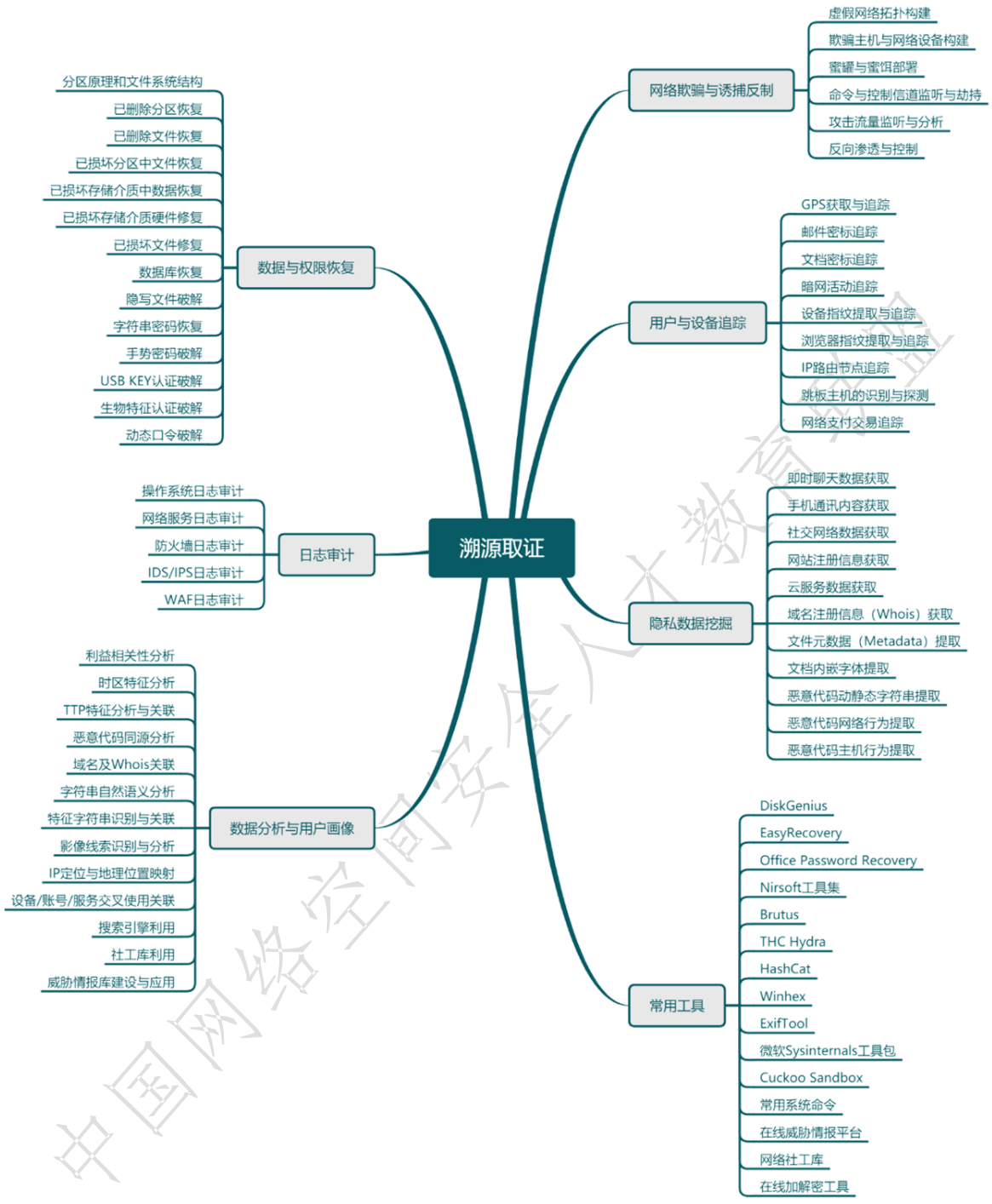
7. 溯源取证知识技术体系

溯源取证作为应对网络攻击的重要环节，在威慑网络攻击和打击网络犯罪方面具有重要意义。从知识技能视角可将溯源取证划分为数据与权限恢复、网络欺骗与诱捕反制、日志审计、用户与设备追踪、隐私数据挖掘、数据分析与用户画像、工具使用等。

（1）数据和权限恢复

数据和权限恢复是一种在攻击者非配合甚至故意破坏的情况下，访问其存储介质、物理设备、网络服务的取证技术手段。数据恢复的目的是找回已删除文件或数据，甚至恢复磁盘分区中全部遭到破坏的数据，在溯源取证中用于应对攻击者对存储介质中文件和数据证据的故意破坏。从基础原理角度，数据恢复技能需要掌握磁盘分区原理和文件系统结构；从技术应用角度，需要掌握的技术还包括已删除分区恢复、已删除文件恢复、已损坏分区中文件恢复、已损坏存储介质中数据恢复、已损坏存储介质硬件恢复、已损坏文件修复、数据库恢复。权限恢复的目的是通过技术手段，在所有者非配合情况下突破用户身份认证措施从而获得设备、文件、数据和服务的访问权限。权限恢复知识技能包括隐写文件破解、字符串密码恢复、手势密码恢复、动态口令破解、生物特征认证破解以及 USB KEY 认证破解。

 ©2019 中国网络空间安全人才教育联盟



中国网络空间安全人才教育联盟

（2）网络欺骗与诱捕反制

网络攻击使用的各类基础设施及攻击针对的目标是溯源取证的重要着眼点，因此诱捕反制是一种高效的溯源取证手段，但是可能涉及司法有效性问题。网络欺骗技术由传统蜜罐演化而来，被定义

 ©2019 中国网络空间安全人才教育联盟

为使用骗局或者假动作来误导攻击行为，能够有效地诱捕网络攻击，从而更好地为溯源取证创造条件。虚假网络拓扑构建、欺骗主机与网络设备构建、蜜罐与蜜饵部署是构建网络欺骗基础环境的必备技能；命令与控制信道监听与劫持、攻击流量监听分析、反向渗透与控制则是较为通用的网络攻击诱捕反制技能，不仅可以在欺骗环境中实施，也可以在常规环境中实施。

（3）日志审计

通过审计各类日志可以发现网络攻击留下的时间、活动、IP 地址、漏洞利用代码、账号等线索，从而分析出网络攻击大致的源头和过程。该部分技能主要包括受害者设备和网络安全设备两类日志的审计，具体包括系统日志审计、网络服务日志审计、防火墙日志审计、IDS/IPS 日志审计和 WAF 日志审计等。

（4）用户与设备追踪

用户与设备追踪主要解决两方面问题：第一，建立攻击者各网络身份、真实身份、设备和攻击事件间的交叉关联关系，并形成持续稳定追踪以刻画整个攻击过程甚至揭露攻击者的真实身份；第二，追踪攻击行为本身及附加行为所产生的网络痕迹，以发现其与攻击者真实身份的关联线索。该部分的技术包括多类型文档蜜标追踪、邮件蜜标追踪、暗网活动追踪、浏览器指纹提取与追踪、设备指纹提取与追踪、GPS 获取与追踪、IP 路由节点追踪、跳板主机的识别与探测、网络支付交易追踪等。

（5）隐私数据挖掘

溯源取证过程中可主动挖掘的隐私数据主要包括四个方面：用户在论坛、社交网络等服务中主动公开的个人数据；网络服务商未采取严格安全措施保护的数据；执法机构采用技术手段或行政手段

 ©2019 中国网络空间安全人才教育联盟

依法获取的数据；攻击者在恶意代码中泄露的隐私数据，合理合法地利用这些数据将对溯源取证产生巨大的帮助。因此，该部分的关键技能包括即时聊天数据获取、手机通讯内容获取、社交网络数据获取、云服务数据获取、域名注册信息（Whois）获取、文档元数据（Metadata）提取、文档内嵌字体提取、恶意代码动静态字符串提取、恶意代码网络行为提取、恶意代码主机行为提取等。

（6）数据分析与用户画像

数据分析与用户画像是溯源攻击者身份最为重要的环节，基于已获取的关键线索，以威胁情报等数据为信息储备，利用大数据、人工智能等技术手段，实现线索溯源与攻击者身份映射，最大程度刻画其身份特征。该部分的技能包括利益相关性分析、TTP 特征分析与关联、时区特征分析、特征字符串发现与关联、恶意代码同源分析、域名及Whois关联、字符串自然语义分析、特征字符串识别与关联、影像线索识别与分析、IP 定位与地理位置映射、设备/账号/服务交叉使用关联、搜索引擎利用、社工库利用、威胁情报库建设与应用。

（更多知识技能体系展开实例在后续版本持续补充更新）

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

附 中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟，是在中国产学研合作促进会的指导下，由从事网络空间安全相关教育、科研、产业、应用的高校、科研学术机构、地方政府、企业单位、社会团体、事业单位和政府机关直（隶）属单位以及热衷于网络空间安全人才教育的个人共同自愿结成的全国性、行业性、非营利性、创新性组织。

联盟旨在发挥桥梁纽带作用，组织和动员全国网安领域顶级高校、企业、事业单位和社会团体，针对人才教育、培养、培训、认证以及就业等环节，探索科学可行的网安人才培养新模式，努力缩小和补齐国家网安人才需求的缺口和短板，为国家网安事业发展提供有力的支撑。

联盟成立于 2018 年 9 月，设理事会、常务理事会和秘书处，共同受会员代表大会监督，在会员代表大会集体授权下，开展工作。联盟下不常设分支机构或分会，根据联盟主旨和当前工作重点，成立了网安人才供需协调工作组、网安人才挖掘发现工作组、网安人才培训培养工作组、网安人才标准认证工作组和网安意识培养提高工作组等主题性工作组。

欢迎有志于网络空间安全人才教育的企业、机构和个人加入！

中国网络空间安全人才教育联盟公众号

 ©2019 中国网络空间安全人才教育联盟