一、应急响应工程师特训班-课前预习内容

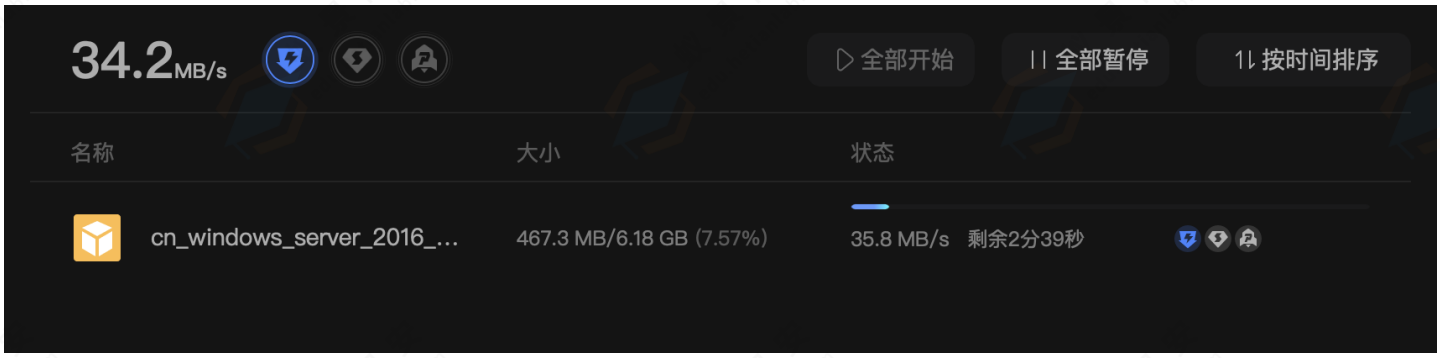
> 可以访问这个链接哦～ https://doc.weixin.qq.com/doc/w3_AYoA2AZ1AEEEuFbf0WETtiBVHKsDm?scode=ADQA_wcYAAsnuPtwTCAYoA2AZ1AEE

1. 必备工具

> - 以下工具只需进行下载和安装即可，无需进行其他额外配置，当然你感兴趣，可以自己先行大胆摸索，对后续课程不会产生任何影响。
> - 以下工具如已安装，均无需替换版本，继续使用自己的就行，不会影响课程学习。
> - 如果有使用M1/M2 Mac的同学，下列工具除Windows Server 2016外，均有替代，例如PD虚拟机。

1. Vmware Workstation Pro 17:
   - 介绍：一款虚拟机软件，可以在上面安装常见的虚拟机
   - 下载链接1（国外官网）：https://www.vmware.com/go/getworkstation-win
   - 下载链接2（百度云）：https://pan.baidu.com/s/1s7k33oldk5ajaqOHlsyCJQ 提取码: q4wr
   - 激活码Key：MC60H-DWHD5-H80U9-6V85M-8280D
   - 教学视频（不推荐看，建议自己操作）：本周更新，先下载好工具
1. Kali：
   - 介绍：一个集成常见网络安全环境与工具的Linux系统，我们学习Linux用他就够了
   - 下载链接1（国外官网） https://cdimage.kali.org/kali-2023.3/kali-linux-2023.3-vmware-amd64.7z
   - 下载链接2（百度云）：https://pan.baidu.com/s/1wOxoS4vHl-ZPUSkgkY2sTQ 提取码: q3hi
   - 教学视频（不推荐看，建议自己操作）：本周更新，先下载好工具
1. Windows Server 2016
   - 介绍：一款服务器版的windows操作系统，是现在服务器主流windows系统
   - 下载链接1（ed2k-迅雷下载）：ed2k://|file|cn_windows_server_2016_x64_dvd_9718765.iso|6176450560|CF1B73D220F1160DE850D9E1979DBD50|/

   > 这里用迅雷下载速度非常快（无需会员）

   - 下载链接2（百度云）： https://pan.baidu.com/s/1ggAbhvAATuJNsG5oA-vwlw?pwd=85og 提取码：85og
   - 激活码Key：CB7KF-BWN84-R7R2Y-793K2-8XDDG
   - 教学视频（不推荐看，建议自己操作）：本周更新，先下载好工具
4. BurpSuite
   - 介绍：一款网络安全常用工具，可以实现对浏览器的中间人攻击，实现拦截请求、抓包等操作
   - 下载链接: https://pan.baidu.com/s/1NsisSVDh-VBPG3u3WWuA?pwd=0ceq
     提取码：0ceq
   - 教学视频（不推荐看，建议自己操作）：本周更新，先下载好工具

2. 必备知识

1. 计算机基本知识
   - 我的电脑配置够吗?
     - 2018 年后主流笔记本电脑、台式机，购入时价格在4000元以上，均能满足课程学习
     - 如果你能看懂配置，那内存16G及以上，硬盘512G及以上，CPU Intel i5、i7、i9 或 AMD r5、 r7 、r9任意系列均能满足课程学习
   - 我要用什么浏览器?
     - Chrome 谷歌浏览器：全球使用量最高的浏览器（你常听说的 360浏览器、QQ浏览器、搜狗浏览器、2345浏览器、百度浏览器都是用Chrome浏览器内核改的）
     - Chrome 下载地址： https://www.google.com/chrome/
     - 说明：如果你刚开始使用Chrome，可能不太习惯，因为他不像国内浏览器有网址导航，你需要在网站栏输入 https://www.baidu.com 才能访问百度。如果你真的离不开国内那套网址导航，访问 https://www.hao123.com/ 就行了。
   - 常见文件后缀名

    - 常用文件扩展名_百度百科
    - https://baike.baidu.com/item/%E5%B8%B8%E7%94%A8%E6%96%87%E4%BB%B6%E6%89%A9%E5%B1%95%E5%90%8D/10227127
    - 记住，不是所有的文件都能双击打开，也不是所有的文档都能用wps打开。
- 我的电脑要怎么浏览PDF，怎么解压软件，怎么打开.md文件 ，怎么截图?
    - 浏览PDF：Chrome谷歌浏览器不仅仅是网站浏览器，也是非常强的多媒体资源阅读器和解码器，PDF更不在话下
    - 解压软件：系统自带的解压软件（不论是Windows还是MacOS）兼容性极差，速度极慢，基本不可用。推荐bandizip https://www.bandisoft.com/bandizip/
    - markdown阅读器：.md文件被称为markdown，需要用支持markdown语法的编辑器才能打开，例如 Typora https://typora.io/。 且几乎所有的编辑代码的IDE都支持阅读.md文件，如 VSC Visual Studio Code - https://code.visualstudio.com/、jetbrains系列所有的IDE（Pycharm、IDEA、PHPStrom、goland）均支持。
    - 截图软件（不要再对屏幕拍照啦）： Snipaste https://www.snipaste.com/

1. 网络基础知识

- IP地址：
    - IP地址是互联网计算机之间的唯一寻址方式，类似收快递与外卖的家庭地址
    - 网络安全视角下，我们必须要分清公网IP和内网IP，其实很简单
        - 内网IP：经过运营商路由器或者自己家的路由器重新分配的局域网，使用命令行ipconfig看到的，如 192.168. 开头、172.16.开头 的IP地址
        - 公网IP：互联网IP，因为IP地址的稀缺性，移动联通电信是不可能给家庭用户直接用公网IP的，一般是一栋楼，甚至一个小区公用同一个互联网IP，查询自己的互联网IP可以使用 https://www.ip138.com/

1. IT行业基础知识

- 常见编程语言
    - 菜鸟教程 - https://www.runoob.com/ 就是菜鸟教程的首页，不要分别点开去看，因为你知道这个世界上都有哪些编程语言和这些编程语言都是干啥的，比你学会一门编程语言对网络安全的积极影响更大
    - 举个例子
        - 例如你看了这部分

        数据库

        你能够知道常见的数据库有 mysql、postgresql、sqlite、mongodb、redis、memcached ，有这些认知，比你去花一周的时间看完【学习MySQL】更有效

- 常见操作系统
    - 世界上的系统分为两类，分别是 Windows 和 Linux（专业称法为 类Unix）
        - Windows： 个人电脑 Windows 10 、Windows 7、Windows XP ，服务器 Windows Server 2008 R2、Windows Server 2016
        - Linux： Ubuntu、Debian、CentOS、Kali、RHEL、统信OS、麒麟OS，Android、MacOS、IOS、鸿蒙OS（后面这四个是 类Unix系统）
- 常见操作系统架构

- 在下载软件的时候，我们必须选择对应的系统版本和系统架构才能运行，例如下面一款常见的网络安全软件Xray，在github的下载页面是这个样子的

▼ Assets 10

sha256.txt	1.14 KB
xray_darwin_amd64.zip	29.2 MB
xray_darwin_arm64.zip	28.5 MB
xray_linux_386.zip	28.1 MB
xray_linux_amd64.zip	29.1 MB
xray_linux_arm64.zip	27.8 MB
xray_windows_386.exe.zip	27.3 MB
xray_windows_amd64.exe.zip	27.9 MB
Source code (zip)	
Source code (tar.gz)	

  - 这里指定的 arm64、amd64、386指定的就是架构
    - x86 （经常用在家用电脑、服务器中）：
      - 32位有386、i386、x86
      - 64位有amd64、i686、x64、x86_64
    - arm （经常用在移动设备、苹果电脑、手机中）：
      - 32位有arm、armv6、armv7
      - 64位有arm64、aarch64、armv8
    - 其他（经常用在工业控制设备中）： 比较少见，比如mips
  - 如果你是使用的正常电脑（Apple M1/M2 芯片电脑除外），你的架构均为 amd64/x86_64 [注意：这里的amd64所指的amd不是CPU生产商amd，即使你使用的Intel I7 处理器，你的架构依然是amd64]
  - 所以综上所述，例如我们使用的是windows 11系统，则下载 xray_windows_amd64.exe.zip ，如果我们使用的是kali，则下载xray_linux_amd64.zip
- 可执行程序的区别
  - 不同系统、不同架构的可执行程序一般不具有兼容性（比如苹果手机不能运行电脑版的英雄联盟，因为一个是windows、一个是ios）
  - windows 的可执行程序后缀为 .exe ， 被称为 PE 文件
  - Linux 的可执行程序后缀为 .elf 或 无后缀，被称为 ELF 文件

3. 推荐书籍

> 书籍请阅读PDF，无需购买实体书籍（买了也是吃灰或者压泡面）
> - 《白帽子讲Web安全》
> - 下载链接：https://pan.baidu.com/s/1gMmM74yos-e1CjDEskgw?pwd=kacr
> - 推荐原因：网络安全国内最有价值的书籍，无数网安大佬的启蒙书，不论你是网络安全入门者，或者是安全从业者，这本书读完将受益匪浅。作者是“道哥”吴翰清，2000年入行网络安全，2005年23岁成为阿里巴巴最年轻的专家，被誉为“阿里守护神”

4. 行业必知

(1) 网络安全法

> 知法懂法、遵纪守法
> - 中华人民共和国网络安全法*滚动新闻*中国政府网
>   - https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
> - 中华人民共和国反间谍法_中国政府网
>   - https://www.gov.cn/yaowen/2023-04/27/content_5753385.htm
> - 关键信息基础设施安全保护条例*信息产业（含电信）*中国政府网
>   - https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

(2) 行业岗位

> 常见行业技术岗位由于企业不同、业务不同，略有差异

- 网络安全产业人才岗位能力要求
  - http://www.miitxxzx.org.cn/module/download/downfile.jsp?classid=0&shownname=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E4%BA%A7%E4%B8%9A%E4%BA%BA%E6%89%8D%E5%B2%97%E4%BD%8D
  - 工信部发布的《网络安全产业人才岗位能力要求》中，4.2 主要岗位及职责 详细列出了网络安全的所有岗位，但由于不同企业人员组织规划有区别，故实际可能有部分差异。

(3) 网安大厂

知道国内有哪些网络安全大企业，对于自己的职业发展尤为重要

2023年中国网安产业竞争力50强

序号	中文简称	企业全称
1	奇安信	奇安信科技集团股份有限公司
2	深信服	深信服科技股份有限公司
3	启明星辰	启明星辰信息技术集团股份有限公司
4	华为	华为技术有限公司
5	天融信	天融信科技集团股份有限公司
6	绿盟科技	绿盟科技集团股份有限公司
7	腾讯	腾讯云计算（北京）有限责任公司
8	新华三	新华三技术有限公司
9	阿里云	阿里云计算有限公司
10	安恒信息	杭州安恒信息技术股份有限公司
11	三六零	三六零数字安全科技集团有限公司
12	亚信安全	亚信安全科技股份有限公司
13	中电科	中电科网络安全科技股份有限公司
14	迪普科技	杭州迪普科技股份有限公司
15	山石网科	山石网科通信技术股份有限公司
16	数字认证	北京数字认证股份有限公司
17	信安世纪	北京信安世纪科技股份有限公司
18	长亭科技	北京长亭科技有限公司
19	安天	安天科技集团股份有限公司
20	美亚柏科	厦门市美亚柏科信息股份有限公司
21	中孚信息	中孚信息股份有限公司
22	观安信息	上海观安信息技术股份有限公司
23	安博通	北京安博通科技股份有限公司
24	青藤云安全	北京升鑫网络科技有限公司
25	永信至诚	北京永信至诚科技股份有限公司
26	三未信安	三未信安科技股份有限公司
27	盛邦安全	远江盛邦（北京）网络安全科技股份有限公司
28	威努特	北京威努特技术有限公司
29	东软	沈阳东软系统集成工程有限公司
30	北信源	北京北信源软件股份有限公司
31	恒安嘉新	恒安嘉新（北京）科技股份公司
32	吉大正元	长春吉大正元信息技术股份有限公司

33	微步在线	北京微步在线科技有限公司
34	格尔软件	格尔软件股份有限公司
35	长扬科技	长扬科技（北京）有限公司
36	默安科技	杭州默安科技有限公司
37	美创科技	杭州美创科技有限公司
38	安华金和	北京安华金和科技有限公司
39	联软科技	深圳市联软科技股份有限公司
40	任子行	任子行网络技术股份有限公司
41	东方通	北京东方通科技股份有限公司
42	明朝万达	北京明朝万达科技股份有限公司
43	网宿科技	网宿科技股份有限公司
44	海泰方圆	北京海泰方圆科技股份有限公司
45	天地和兴	北京天地和兴科技有限公司
46	博智安全	博智安全科技股份有限公司
47	瑞数信息	瑞数信息技术（上海）有限公司
48	斗象信息	上海斗象信息科技有限公司
49	芯盾时代	北京芯盾时代科技有限公司
50	珞安科技	北京珞安科技有限责任公司

5. 常见问题

1. 我如何参加蓝队实战?
   - 参加hw，国家级HW、省市级HW、行业HW和各种重保、演练都可以
   - 参加CTF比赛 （现今的网络安全比赛，防御、蓝队类赛事和题型越来越多，参考实景防御赛(Real Defense Game/RDG)、电子数据取证大赛等，国家级的安全比赛都有安全防御类赛题）
   - 如果你没有任何安全基础，还是建议先把课程学好
2. 我有必要学习攻击方向的安全知识吗?
   - 如果你想进入网络安全大厂成为一名合格的网安从业者，或者不想止步于蓝队初级或中级，就需要
3. 如果我想学，该如何学习攻击方向安全知识?
   - 看上文推荐的安全书籍
   - 打靶场
     - 初、中级靶场：DVWA，打完这个常见的漏洞就会了，可以顺利进行漏洞挖掘，或成为一名安全服务工程
     - 高级靶场：https://portswigger.net/web-security/all-labs ， 这是BurpSuite的官方靶场，有些难度非常高，对新手非常不友好，可以当做长期目标，慢慢攻破
     - 内网渗透高级靶场：Hack The Box: https://www.hackthebox.com/， HTB靶场，综合内网，收费很贵，对新手极其不友好，不建议入门者尝试，且有些难度非常高，可以当做长期目标
   - 挖漏洞
     - SRC导航 https://www.anquanke.com/src
     - 对新手比较友好
       - 教育SRC：https://src.sjtu.edu.cn/
       - 漏洞盒子：https://www.vulbox.com/
       - 补天：https://www.butian.net/
   - 学习蚁景网安系统性教程
     - Web安全
     - 渗透测试
     - 全栈安全开发

> 详情咨询班主任 奶茶～ 旺仔～

4. 我有必要学习编程语言吗？如果有，学习哪种编程语言比较好?
   - 如果你有时间且感兴趣，可以学。不学，对应急响应蓝队也无大影响。
   - 学Python，简单易上手，对网络安全帮助很大。其他语言对网络安全帮助很小。

> - 推荐网站 Python教程 - 廖雪峰的官方网站 https://www.liaoxuefeng.com/wiki/1016959663602400（如果你能把这个网站的70%内容掌握[如果你有耐心，一个星期时间完全足够]，你的编程技术已经超越了至少80%以上的在职网络安全工程师