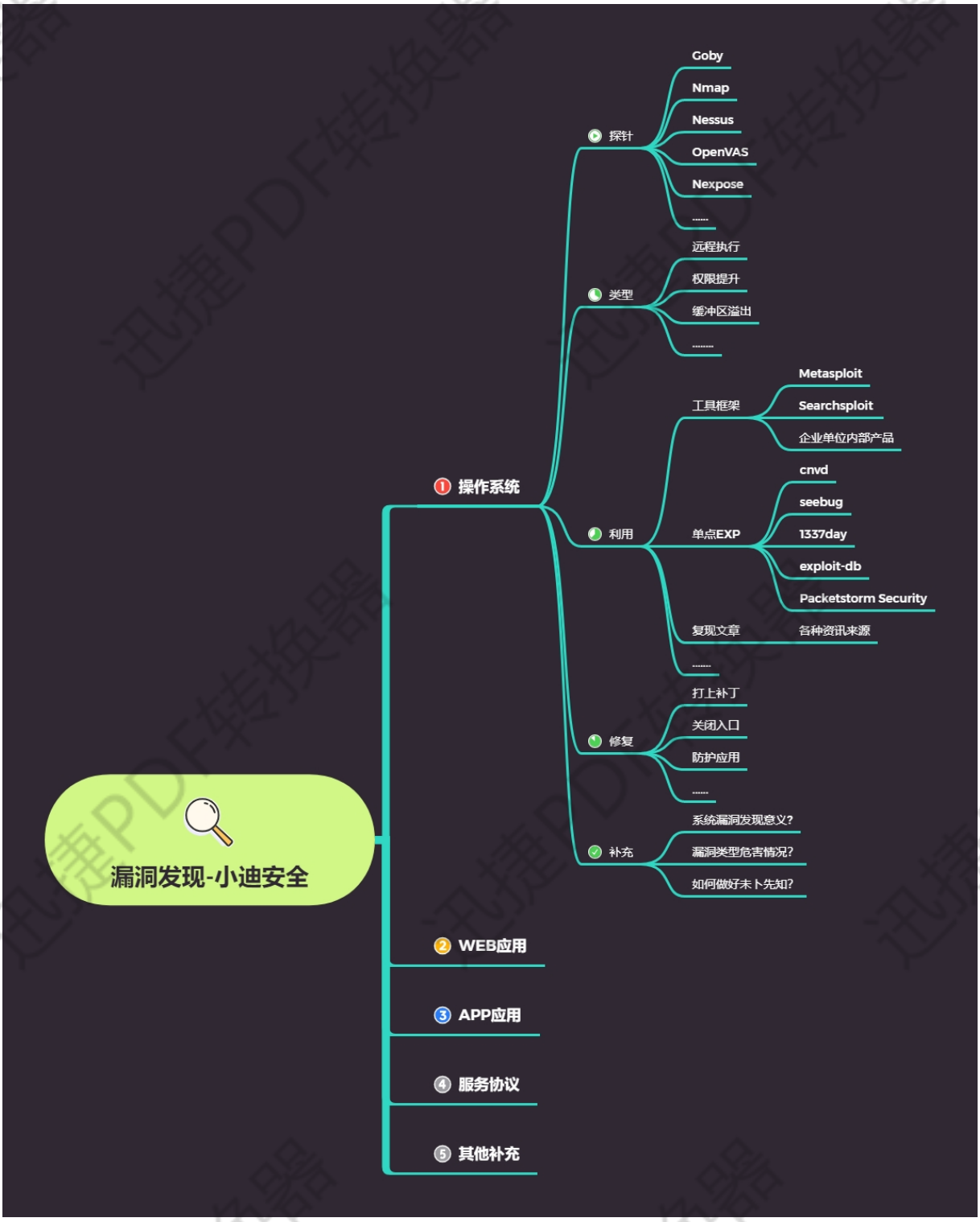
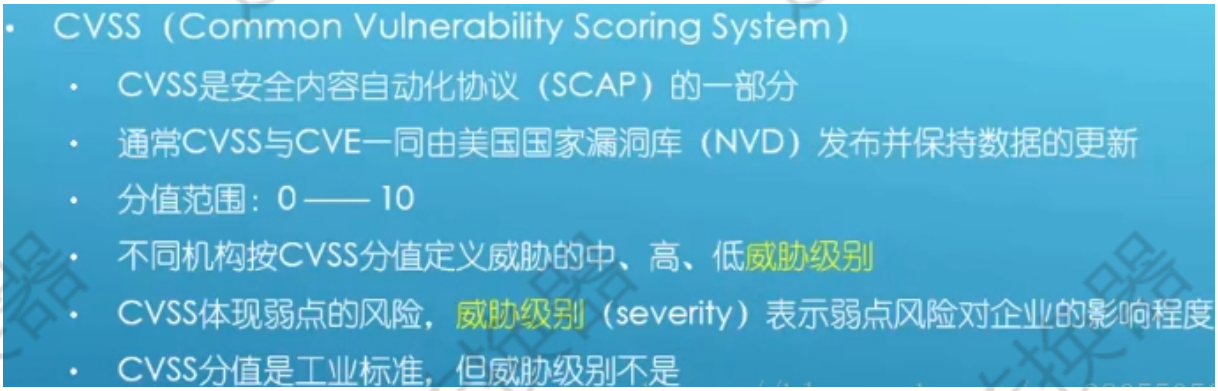
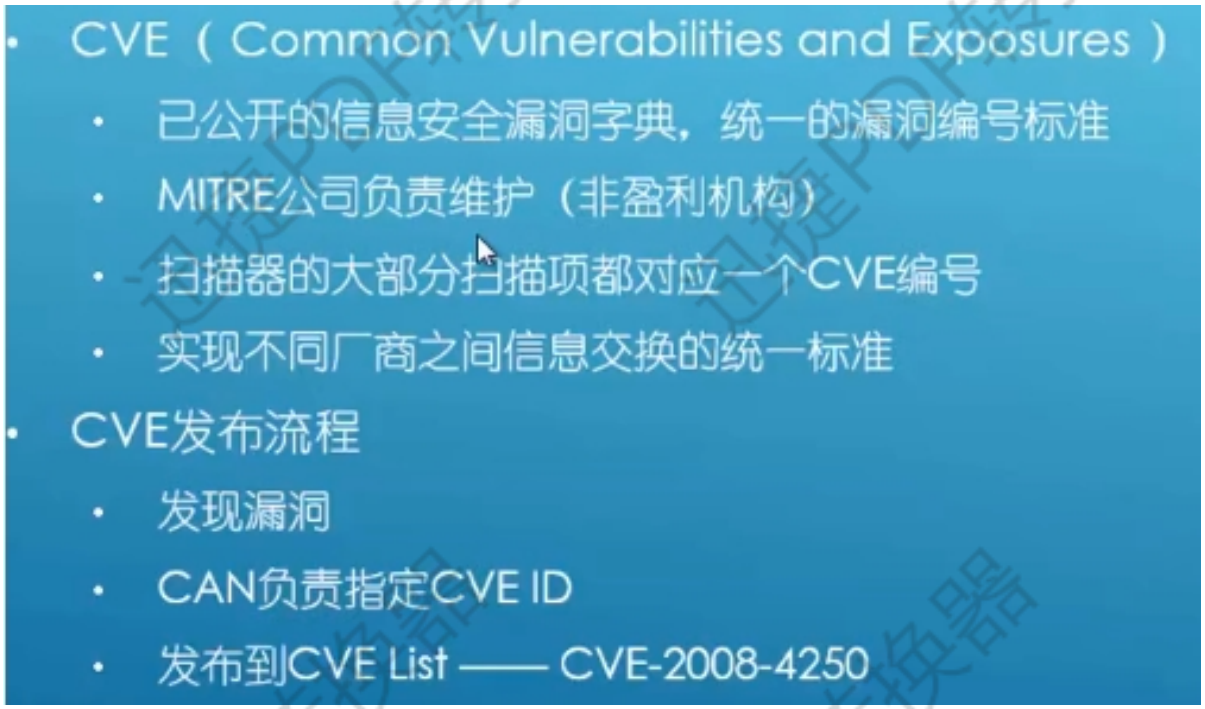
漏洞发现-操作系统之漏洞探针类型利用修复







演示案例：

➢ 漏洞扫描工具演示-Goby,Nmap,Nessus(操作)

#Goby,Nmap,Nessus
Goby 忍者系统测试
Nmap --script=vuln 默认 nse 插件
Nmap vulscan vulners 调用第三方库探针
https://www.cnblogs.com/shwang/p/12623669.html
Nessus 安装-使用-插件库加载扫描

#安装 nessus 执行命令的时候一定要管理员运行执行

➢ 漏洞类型区分讲解-权限提升,远程执行等(思路)

➢ 漏洞利用框架演示-Metasploit,Searchsploit 等(操作)

#CVE-2019-0708 MS12-020 - 牛逼忍者系统全程测试
https://www.jianshu.com/p/bd8213c53717
-c, --case[Term]执行区分大小写的搜索，缺省是对大小写不敏感。
-e, --exact [Term]对 exploit 标题执行 EXACT 匹配（默认为 AND）
-h, --help 在屏幕上显示帮助
-j, --json[Term]以 JSON 格式显示结果
-m, --mirror [EDB-ID]将一个漏洞利用镜像（副本）到当前工作目录，后面跟漏洞 ID 号
-o, --overflow [Term]Exploit 标题被允许溢出其列
-p, --path[EDB-ID]显示漏洞利用的完整路径（如果可能，还将路径复制到剪贴板），后面跟漏洞 ID 号
-t, --title[Term]仅仅搜索漏洞标题（默认是标题和文件的路径）
-u, --update 检查并安装任何 exploitdb 软件包更新（deb 或 git）
-w, --www [Term]显示 Exploit-DB.com 的 URL 而不是本地路径（在线搜索）
-x, --examine[EDB-ID]使用$ PAGER 检查（副本）漏洞利用
--colour 在搜索结果中禁用颜色突出显示.
--id 显示 EDB-ID 值而不是本地路径
--nmap[file.xml]使用服务版本检查 Nmap XML 输出中的所有结果（例如：nmap -sV -oX file.xml）。
使用“-v”（详细）来尝试更多的组合
--exclude="term"从结果中删除值。通过使用“|”分隔多个值，例如--exclude
=“term1 | term2 | term3”

```
Usage: searchsploit [options] term1 [term2] ... [termN] ==========
 Examples
==========
  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446 searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/" For more examples, see the manual: h
ttps://www.exploit-db.com/searchsploit/ =========
 Options
=========
   -c, --case [Term]      区分大小写(默认不区分大小写)
   -e, --exact    [Term]      对exploit标题进行EXACT匹配 (默认为 AND) [Implies "-t"].
   -h, --help                 显示帮助
   -j, --json     [Term]      以JSON格式显示结果
   -m, --mirror   [EDB-ID]    把一个exp拷贝到当前工作目录,参数后加目标id
   -o, --overflow [Term]      Exploit标题被允许溢出其列
   -p, --path     [EDB-ID]    显示漏洞利用的完整路径（如果可能，还将路径复制到剪贴板），后面跟漏洞ID号
   -t, --title    [Term]      仅仅搜索漏洞标题（默认是标题和文件的路径）
   -u, --update               检查并安装任何exploitdb软件包更新（deb或git）
   -w, --www      [Term]      显示Exploit-DB.com的URL而不是本地路径（在线搜索）
   -x, --examine  [EDB-ID]    使用$ PAGER检查（副本）Exp
       --colour               搜索结果不高亮显示关键词
       --id                   显示EDB-ID
       --nmap     [file.xml]  使用服务版本检查Nmap XML输出中的所有结果（例如：nmap -sV -oX file.xml）
                                使用“-v”（详细）来尝试更多的组合
       --exclude="term" 从结果中删除值。通过使用“|”分隔多个值
                              例如--exclude=“term1 | term2 | term3”。

=======
 Notes
=======
 * 你可以使用任意数量的搜索词。
 * Search terms are not case-sensitive (by default), and ordering is irrelevant.
   * 搜索术语不区分大小写(默认情况下)，而排序则无关紧要。
   * 如果你想用精确的匹配来过滤结果，请使用用 -e 参数
 * 使用' - t '将文件的路径排除，以过滤搜索结果
   * 删除误报(特别是在搜索使用数字时 - i.e. 版本).
 * 当更新或显示帮助时，搜索项将被忽略。
```

➢ 漏洞修复方案讲解说明-补丁,防护软件,手工修复等(操作及思路)

涉及资源：

https://nmap.org

https://gobies.org

https://www.cnvd.org.cn

https://www.seebug.org

https://www.exploit-db.com

https://github.com/scipag/vulscan

https://github.com/vulnersCom/nmap-vulners

https://github.com/offensive-security/exploitdb

https://www.cnblogs.com/shwang/p/12623669.html

https://blog.csdn.net/qq_38055050/article/details/80214684

https://pan.baidu.com/s/17uA2OmJbV_cDG2C6QnHqqA 提取码：

cxd4
