

Day75 漏洞利用-MSF 框架 &CVE&CNVD&POC&EXP 监控&查找&整 理

漏洞发现-小迪安全

1 WEB/框架

- 1、Burp
 - 配合抓包
 - 联动其他工具
- 2、Xray
 - 内部版社区版
 - 主动扫描
 - 被动扫描
- 3、Awvs
 - 所有暴露资产特扫
- 4、Goby
 - 所有暴露资产特扫
 - 插件多可联动
- 5、Afrog
 - 常见web及框架特扫
 - pocassist升级版
- 6、Vulmap
 - 常见web及框架特扫
- 7、Pocassist
 - 学习思路DIY POC

2 APP/小程序

- 浏览器插件
 - fofa_view
 - Hack-Tools
 - pentestkit
- BurpSuite插件
 - Fiora
 - SpringScan
 - FastjsonScan
 - Log4j-check
 - BurpShiroPassiveScan
 - nuclei-burp-plugin

3 操作系统

- Goby
 - 所有暴露资产特扫
 - Nuclei
 - Fofamap
 - POC多
 - Nessus
 - Nexpose
 - 联动MSF
- 操作系统特扫

4 漏洞利用

- 漏洞编号
 - CVE
 - CNVD
- 查找库
 - 项目
 - Poc-in-github
 - exploitdb
 - 信息
 - 编号
 - 对象名
 - 类型&端口等
- 整理库
 - 项目
 - CNVD监控
 - CVE监控
 - 完善
 - 最新漏洞监控
 - 实现关键字漏洞情况
- 利用框架
 - MSF
 - 特定图形化渗透武器库

1.知识点

- 1、MSF-漏洞利用框架使用
- 2、库查找-CVE&CNVD&关键字
- 3、库整理-CVE&CNVD 漏洞详情
- 4、新漏洞-框架或其他未集成利用

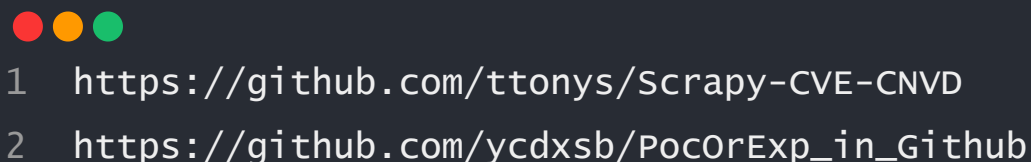
集成和未集成漏洞的利用思路，漏洞利用条件等。

2.漏洞资源

- today-cve https://cassandra.cerias.purdue.edu/CVE_changes/today.html
 - cve 官网 <https://cve.mitre.org/>
 - 国家信息安全漏洞共享平台 <https://www.cnvd.org.cn/>
 - 国家信息安全漏洞库 <http://www.cnnvd.org.cn/>
-

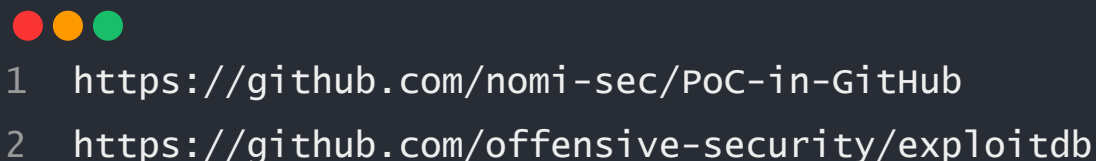
3.演示案例

3.1 漏洞利用-整理库-PocOrExp&CVE-CNVD



```
1 https://github.com/ttonys/Scrapy-CVE-CNVD
2 https://github.com/ycdxsb/PocOrExp_in_Github
```

3.2 漏洞利用-查找库-SearchSploit&PoC-in-GitHub



```
1 https://github.com/nomi-sec/PoC-in-GitHub
2 https://github.com/offensive-security/exploitdb
```

3.3 漏洞利用-模块框架-MetaSploit-Framework (MSF)



- 1 <https://www.metasploit.com/>
- 2 安装下载:
- 3 <https://docs.metasploit.com/docs/using-metasploit/gettingstarted/nightly-installers.html>
- 4 简单使用:
- 5 https://blog.csdn.net/weixin_42380348/article/details/123549631

3.4 漏洞利用-杂乱工具-特定图像化渗透武器库 (V6.1)



- 1 <https://mp.weixin.qq.com/s/Ha1R17KH-vssbr8cmYw14Q>