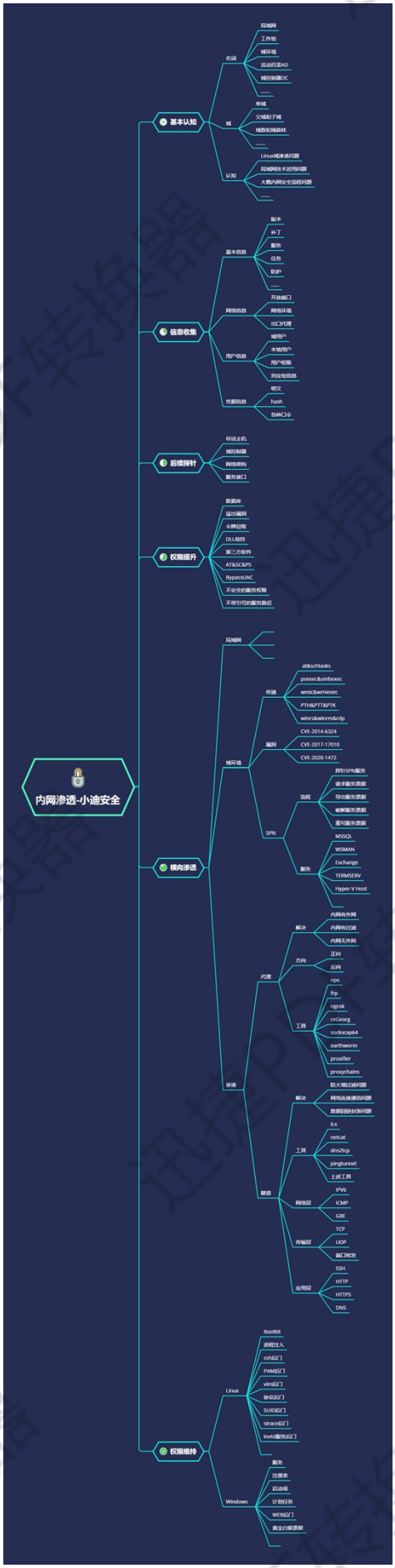
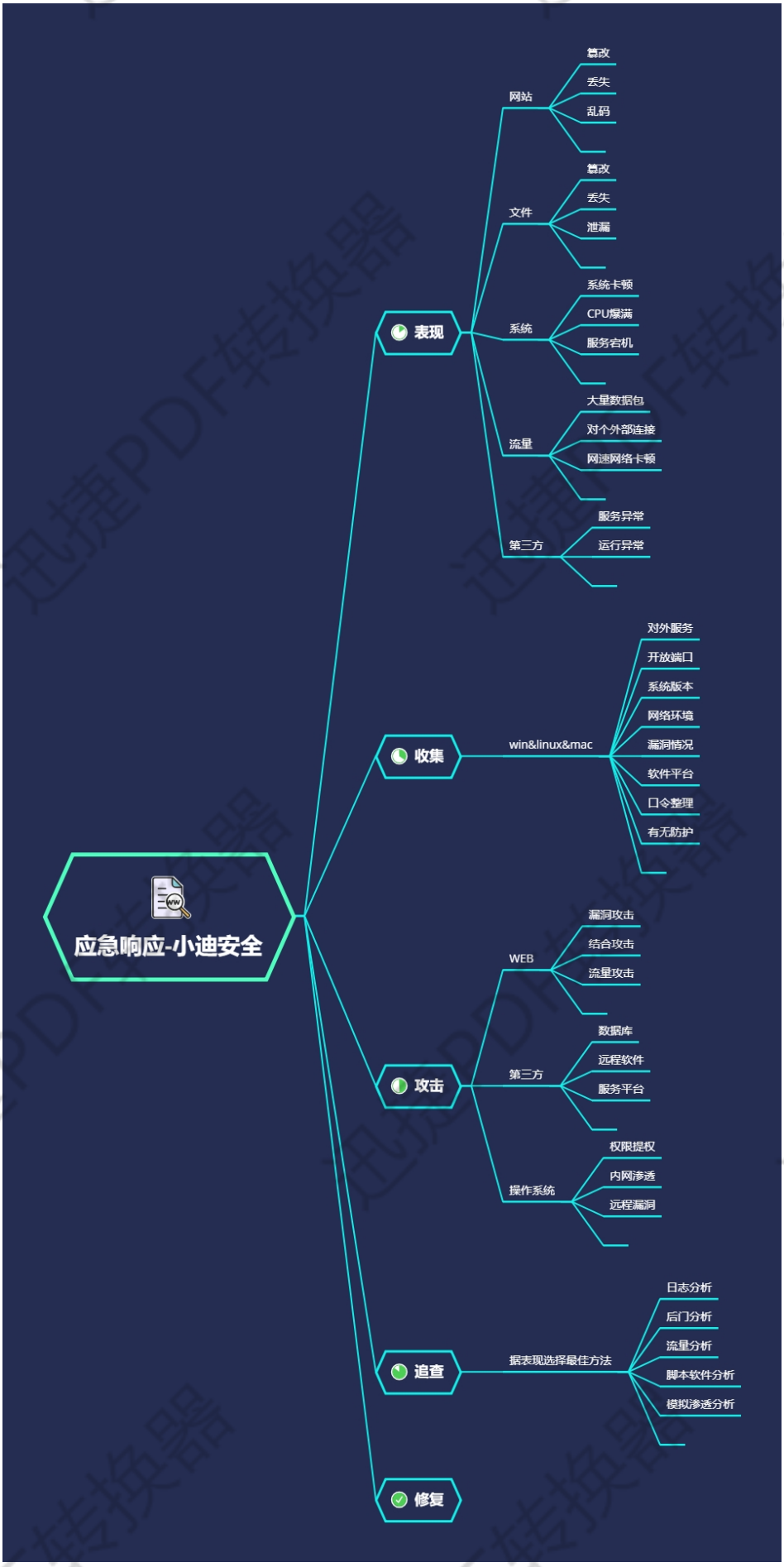
内网安全-域横向 CS&MSF 联动及应急响应初识


内网渗透-小迪安全
基本认知
在园
局域网
工作组
域环境
活动目录AD
域控制器DC
.....
域
单域
父域和子域
域数和域森林
.....
认知
Linux域渗透问题
局域网技术应用问题
大型内网安全流程问题
.....
信息收集
基本信息
版本
补丁
服务
任务
启护
.....
网络信息
开放端口
网络环境
出口代理
用户信息
域用户
本地用户
用户权限
其他组织信息
凭据信息
明文
hash
各种口令
后续探针
存活主机
域控制器
网络架构
服务端口
权限提升
数据库
监控漏洞
令牌窃取
DLL劫持
第三方软件
AT&SC&PS
BypassUAC
不安全的服务权限
不带引号的服务路径
横向渗透
局域网
域环境
传递
at&schtasks
psexec&smbexec
wmic&wmiexec
PTH&PTT&PTK
winrs&winrm&rdp
漏洞
CVE-2014-6324
CVE-2017-17010
CVE-2020-1472
SPN
流程
探针SPN服务
请求服务票据
导出服务票据
破解服务票据
重写服务票据
服务
MSSQL
WSMAN
Exchange
TERMSERV
Hyper-V Host
穿透
代理
解决
内网有外网
内网有过滤
内网无外网
方向
正向
反向
工具
nps
frp
ngrok
reGeorg
sockscap64
earthworm
proxifier
proxychains
隧道
解决
防火墙拦截问题
网络连接通信问题
数据回显封装问题
工具
lcx
netcat
dns2tcp
pingtunnel
上述工具
网络层
IPV6
ICMP
GRE
传输层
TCP
UDP
端口转发
应用层
SSH
HTTP
HTTPS
DNS
权限维持
Linux
Rootkit
进程注入
ssh后门
PAM后门
vim后门
协议后门
SUID后门
strace后门
inetd服务后门
Windows
服务
注册表
启动组
计划任务
WEB后门
黄金白银票据


应急响应-小迪安全
表现
网站
篡改
丢失
乱码
文件
篡改
丢失
泄漏
系统
系统卡顿
CPU爆满
服务宕机
流量
大量数据包
对个外部连接
网速网络卡顿
第三方
服务异常
运行异常
收集
win&linux&mac
对外服务
开放端口
系统版本
网络环境
漏洞情况
软件平台
口令整理
有无防护
攻击
WEB
漏洞攻击
结合攻击
流量攻击
第三方
数据库
远程软件
服务平台
操作系统
权限提权
内网渗透
远程漏洞
追查
据表现选择最佳方法
日志分析
后门分析
流量分析
脚本软件分析
模拟渗透分析
修复

演示案例：

- MSF&CobaltStrike 联动 Shell
- WEB 攻击应急响应朔源-后门,日志
- WIN 系统攻击应急响应朔源-后门,日志,流量
- 临时给大家看看学的好的怎么干对应 CTF 比赛

涉及资源：

https://www.onlinedown.net/soft/628964.htm

https://www.cnblogs.com/xiaozi/p/12679777.html

http://www.pc6.com/softview/SoftView_195167.html

https://github.com/EricZimmerman/AppCompatCacheParser/releases/