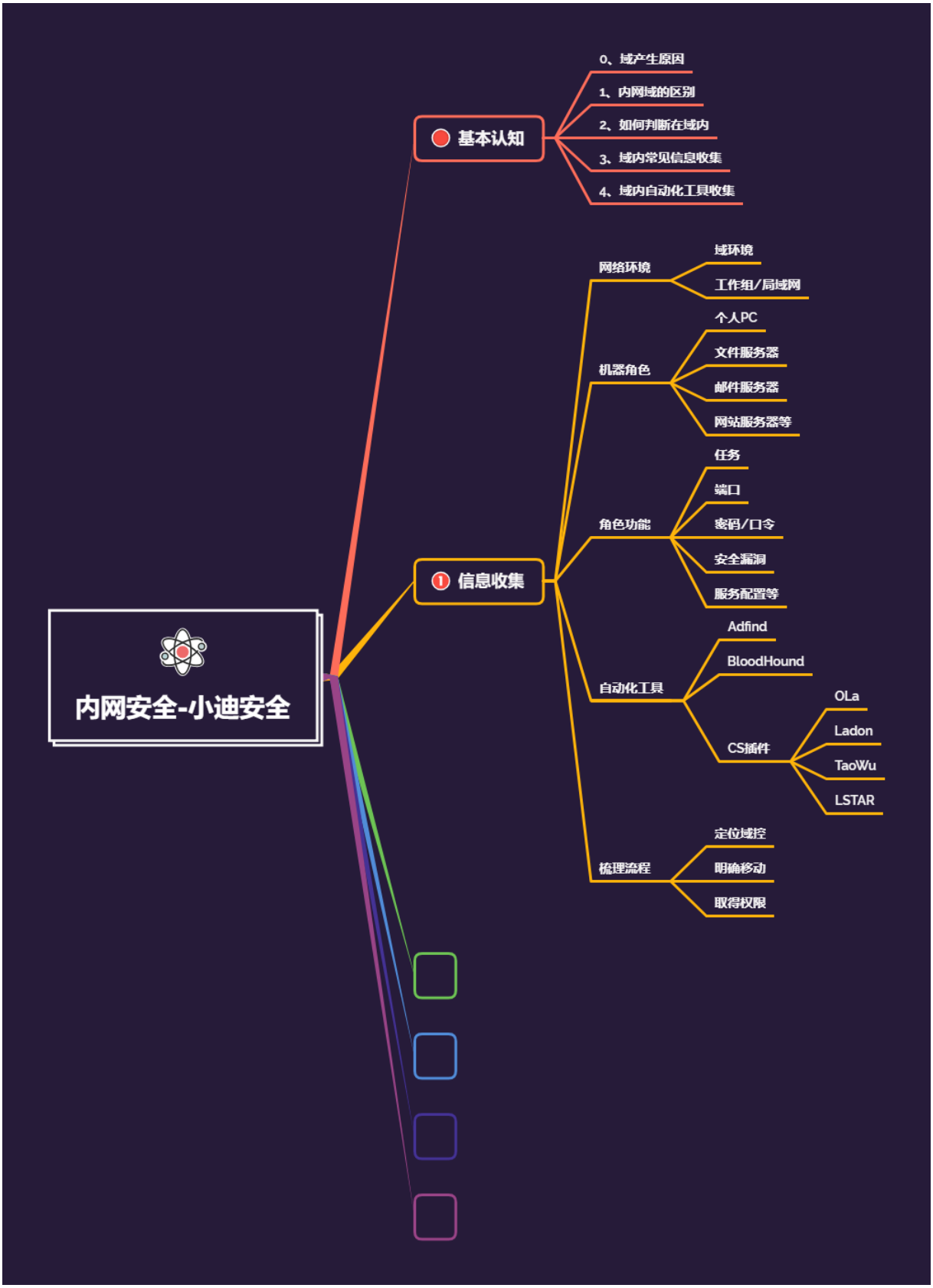
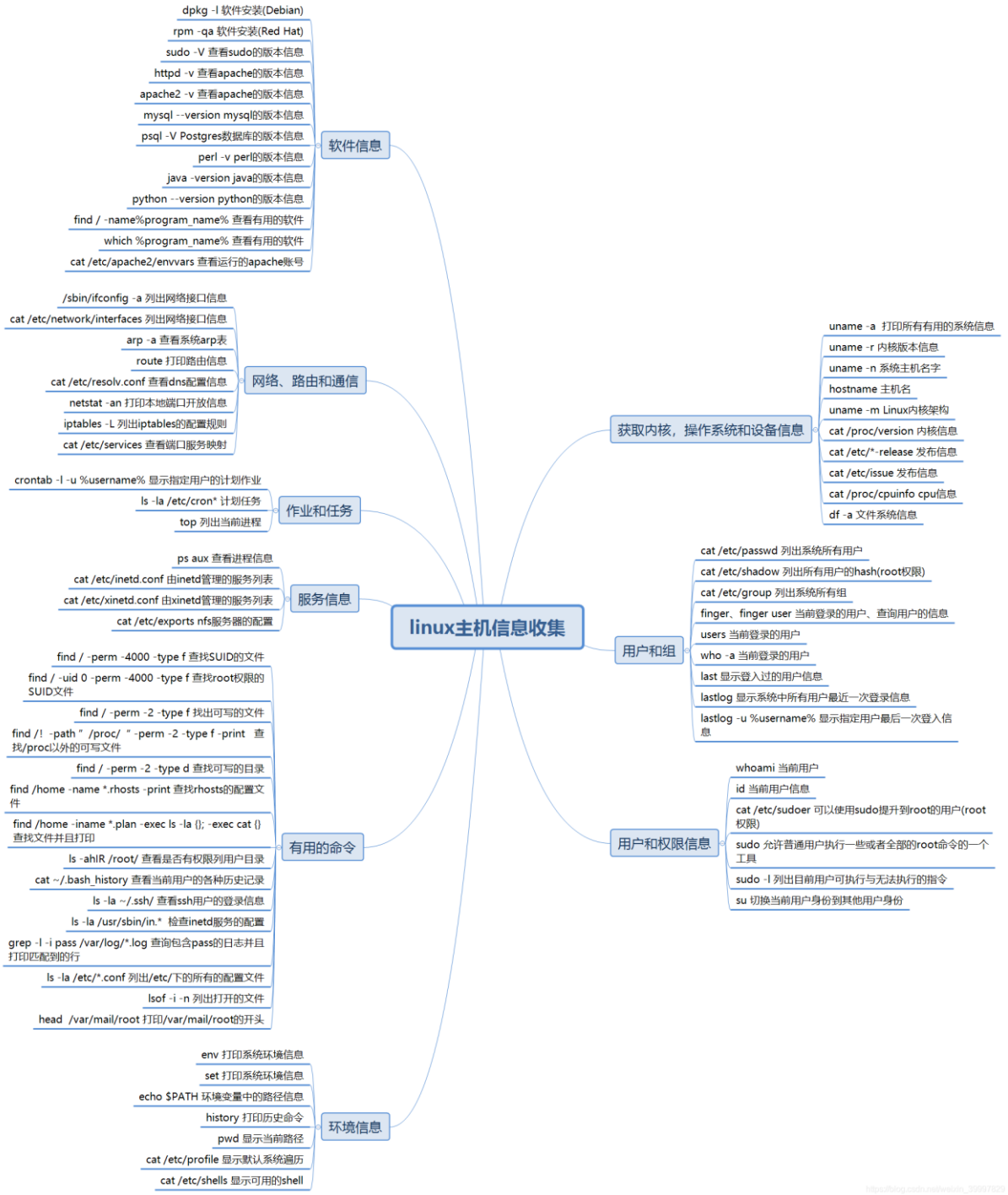
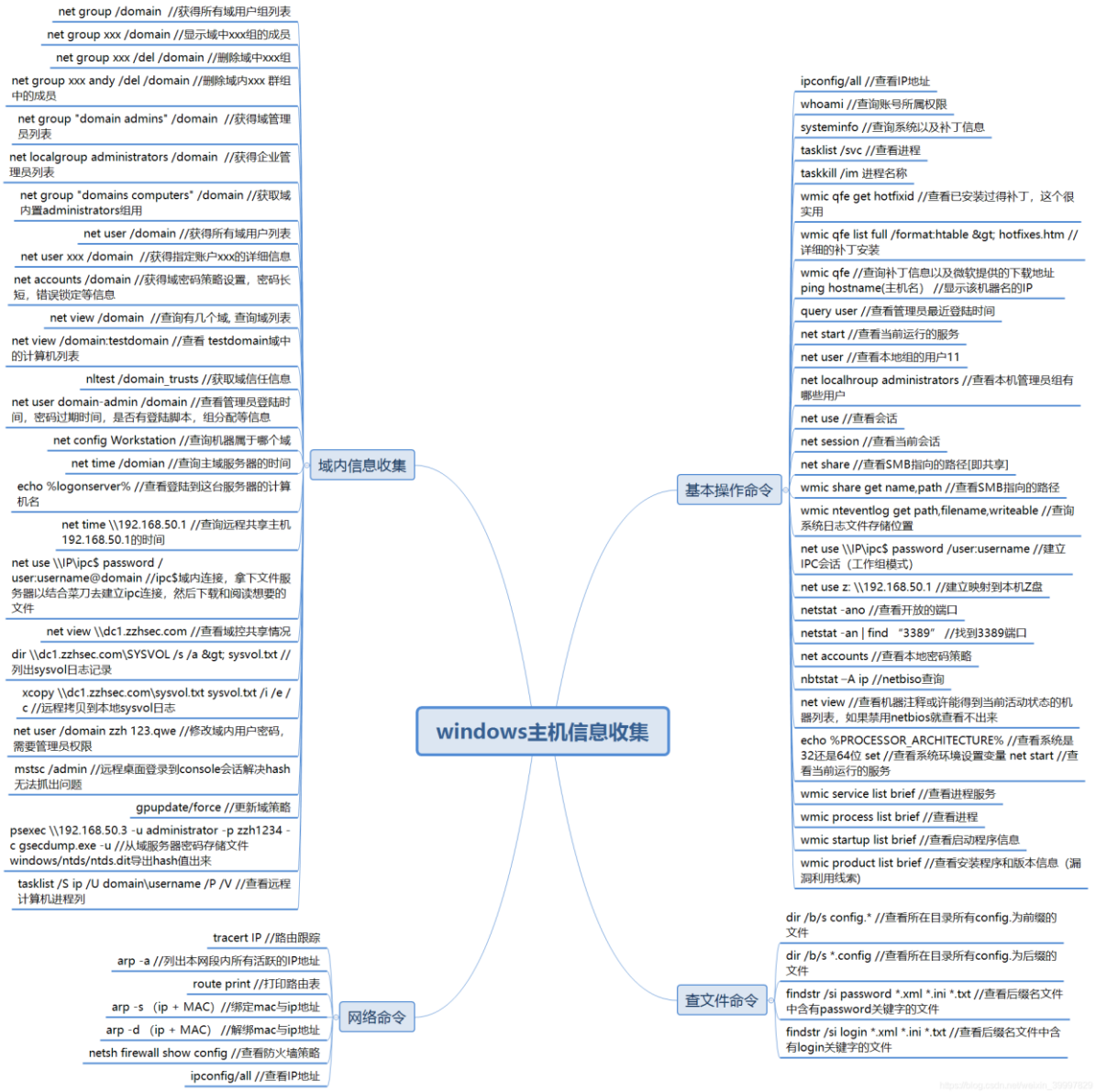
内网安全-域信息收集&应用网络凭据&CS 插件&Adfind&BloodHound




linux主机信息收集
软件信息
dpkg -l 软件安装(Debian)
rpm -qa 软件安装(Red Hat)
sudo -V 查看sudo的版本信息
httpd -v 查看apache的版本信息
apache2 -v 查看apache的版本信息
mysql --version mysql的版本信息
psql -V Postgres数据库的版本信息
perl -v perl的版本信息
java -version java的版本信息
python --version python的版本信息
find / -name%program_name% 查看有用的软件
which %program_name% 查看有用的软件
cat /etc/apache2/envvars 查看运行的apache账号
网络、路由和通信
/sbin/ifconfig -a 列出网络接口信息
cat /etc/network/interfaces 列出网络接口信息
arp -a 查看系统arp表
route 打印路由信息
cat /etc/resolv.conf 查看dns配置信息
netstat -an 打印本地端口开放信息
iptables -L 列出iptables的配置规则
cat /etc/services 查看端口服务映射
作业和任务
crontab -l -u %username% 显示指定用户的计划作业
ls -la /etc/cron* 计划任务
top 列出当前进程
服务信息
ps aux 查看进程信息
cat /etc/inetd.conf 由inetd管理的服务列表
cat /etc/xinetd.conf 由xinetd管理的服务列表
cat /etc/exports nfs服务器的配置
有用的命令
find / -perm -4000 -type f 查找SUID的文件
find / -uid 0 -perm -4000 -type f 查找root权限的SUID文件
find / -perm -2 -type f 找出可写的文件
find /! -path " /proc/ " -perm -2 -type f -print 查找/proc以外的可写文件
find / -perm -2 -type d 查找可写的目录
find /home -name *.rhosts -print 查找rhosts的配置文件
find /home -iname *.plan -exec ls -la {}; -exec cat {} 查找文件并且打印
ls -ahlR /root/ 查看是否有权限列用户目录
cat ~/.bash_history 查看当前用户的各种历史记录
ls -la ~/.ssh/ 查看ssh用户的登录信息
ls -la /usr/sbin/in.* 检查inetd服务的配置
grep -l -i pass /var/log/*.log 查询包含pass的日志并且打印匹配到的行
ls -la /etc/*.conf 列出/etc/下的所有的配置文件
lsof -i -n 列出打开的文件
head /var/mail/root 打印/var/mail/root的开头
环境信息
env 打印系统环境信息
set 打印系统环境信息
echo $PATH 环境变量中的路径信息
history 打印历史命令
pwd 显示当前路径
cat /etc/profile 显示默认系统遍历
cat /etc/shells 显示可用的shell
获取内核，操作系统和设备信息
uname -a 打印所有有用的系统信息
uname -r 内核版本信息
uname -n 系统主机名字
hostname 主机名
uname -m Linux内核架构
cat /proc/version 内核信息
cat /etc/*-release 发布信息
cat /etc/issue 发布信息
cat /proc/cpuinfo cpu信息
df -a 文件系统信息
用户和组
cat /etc/passwd 列出系统所有用户
cat /etc/shadow 列出所有用户的hash(root权限)
cat /etc/group 列出系统所有组
finger、finger user 当前登录的用户、查询用户的信息
users 当前登录的用户
who -a 当前登录的用户
last 显示登入过的用户信息
lastlog 显示系统中所有用户最近一次登录信息
lastlog -u %username% 显示指定用户最后一次登入信息
用户和权限信息
whoami 当前用户
id 当前用户信息
cat /etc/sudoer 可以使用sudo提升到root的用户(root权限)
sudo 允许普通用户执行一些或者全部的root命令的一个工具
sudo -l 列出目前用户可执行与无法执行的指令
su 切换当前用户身份到其他用户身份


windows主机信息收集
域内信息收集
net group /domain //获得所有域用户组列表
net group xxx /domain //显示域中xxx组的成员
net group xxx /del /domain //删除域中xxx组
net group xxx andy /del /domain //删除域内xxx 群组中的成员
net group "domain admins" /domain //获得域管理员列表
net localgroup administrators /domain //获得企业管理员列表
net group "domains computers" /domain //获取域内置administrators组用
net user /domain //获得所有域用户列表
net user xxx /domain //获得指定账户xxx的详细信息
net accounts /domain //获得域密码策略设置，密码长短，错误锁定等信息
net view /domain //查询有几个域, 查询域列表
net view /domain:testdomain //查看 testdomain域中的计算机列表
nltest /domain_trusts //获取域信任信息
net user domain-admin /domain //查看管理员登陆时间，密码过期时间，是否有登陆脚本，组分配等信息
net config Workstation //查询机器属于哪个域
net time /domian //查询主域服务器的时间
echo %logonserver% //查看登陆到这台服务器的计算机名
net time \\192.168.50.1 //查询远程共享主机192.168.50.1的时间
net use \\IP\ipc$ password /user:username@domain //ipc$域内连接，拿下文件服务器以结合菜刀去建立ipc连接，然后下载和阅读想要的文件
net view \\dc1.zzhsec.com //查看域控共享情况
dir \\dc1.zzhsec.com\SYSVOL /s /a > sysvol.txt //列出sysvol日志记录
xcopy \\dc1.zzhsec.com\sysvol.txt sysvol.txt /i /e /c //远程拷贝到本地sysvol日志
net user /domain zzh 123.qwe //修改域内用户密码，需要管理员权限
mstsc /admin //远程桌面登录到console会话解决hash无法抓出问题
gpupdate/force //更新域策略
psexec \\192.168.50.3 -u administrator -p zzh1234 -c gsecdump.exe -u //从域服务器密码存储文件windows/ntds/ntds.dit导出hash值出来
tasklist /S ip /U domain\username /P /V //查看远程计算机进程列
网络命令
tracert IP //路由跟踪
arp -a //列出本网段内所有活跃的IP地址
route print //打印路由表
arp -s （ip + MAC）//绑定mac与ip地址
arp -d （ip + MAC）//解绑mac与ip地址
netsh firewall show config //查看防火墙策略
ipconfig/all //查看IP地址
基本操作命令
ipconfig/all //查看IP地址
whoami //查询账号所属权限
systeminfo //查询系统以及补丁信息
tasklist /svc //查看进程
taskkill /im 进程名称
wmic qfe get hotfixid //查看已安装过得补丁，这个很实用
wmic qfe list full /format:htable > hotfixes.htm //详细的补丁安装
wmic qfe //查询补丁信息以及微软提供的下载地址
ping hostname(主机名） //显示该机器名的IP
query user //查看管理员最近登陆时间
net start //查看当前运行的服务
net user //查看本地组的用户11
net localhroup administrators //查看本机管理员组有哪些用户
net use //查看会话
net session //查看当前会话
net share //查看SMB指向的路径[即共享]
wmic share get name,path //查看SMB指向的路径
wmic nteventlog get path,filename,writeable //查询系统日志文件存储位置
net use \\IP\ipc$ password /user:username //建立IPC会话（工作组模式）
net use z: \\192.168.50.1 //建立映射到本机Z盘
netstat -ano //查看开放的端口
netstat -an | find “3389” //找到3389端口
net accounts //查看本地密码策略
nbtstat -A ip //netbiso查询
net view //查看机器注释或许能得到当前活动状态的机器列表，如果禁用netbios就查看不出来
echo %PROCESSOR_ARCHITECTURE% //查看系统是32还是64位 set //查看系统环境设置变量 net start //查看当前运行的服务
wmic service list brief //查看进程服务
wmic process list brief //查看进程
wmic startup list brief //查看启动程序信息
wmic product list brief //查看安装程序和版本信息（漏洞利用线索）
查文件命令
dir /b/s config.* //查看所在目录所有config.为前缀的文件
dir /b/s *.config //查看所在目录所有config.为后缀的文件
findstr /si password *.xml *.ini *.txt //查看后缀名文件中含有password关键字的文件
findstr /si login *.xml *.ini *.txt //查看后缀名文件中含有login关键字的文件

#知识点：

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

-局域网&工作组&域环境区别

-域环境信息收集-应用&网络&服务&凭据等

-自动化工具使用-CS 插件&Adfind&BloodHound

0x01

一个具有一定规模的企业，每天都可能面临员工入职和离职，因此网络管理部门经常需要对域成员主机进行格式化消除磁盘的文件，然后重装系统及软件，以提供给新员工使用；因此，为了便于后期交接，大多网络管理员会做好一个系统镜像盘，统一安装所有的电脑，并且在安装的时候设置惯用、甚至统一的密码。

0x02

因此，域中的计算机本地管理员账号，极有可能能够登陆域中较多的计算机，本地管理员的密码在服务器上后期修改的概率，远低于在个人办公电脑上的概率，而域用户权限是较低的，是无法在域成员主机上安装软件的，这将会发生下面的一幕：

某个域用户需要使用 viso 软件进行绘图操作，于是联系网络管理员进行安装，网络管理员采用域管理员身份登录了域成员主机，并帮助其安装了 viso 软件，于是这个有计算机基础的员工，切换身份登录到了本地计算机的管理员，后执行 mimikatz，从内存当中抓取了域管理员的密码，便成功的控制了整个域。

0x03

因此，域渗透的思路就是：通过域成员主机，定位出域控制器 IP 及域管理员账号，利用域成员主机作为跳板，扩大渗透范围，利用域管理员可以登陆域中任何成员主机的特性，定位出域管理员登陆过的主机 IP，设法从域成员主机内存中 dump 出域管理员密码，进而拿下域控制器、渗透整个内网。

--当前机器角色的判断

--当前机器网络环境判断

--当前机器角色功能判断

网络环境-局域网&工作组&域环境

机器角色-个人 PC&文件服务器&邮件服务器等

角色功能-任务&端口&服务&密码&漏洞&配置等

演示案例：

- 常规信息类收集-应用&服务&权限等
- 架构信息类收集-网络&用户&域控等
- 关键信息类收集-密码&凭据&口令等
- 自动化工具探针-插件&Adfind&BloodHound

#常规信息类收集-应用&服务&权限等

更多其他收集见上图命令表

systeminfo 详细信息

netstat -ano 端口列表

route print 路由表

net start 启动服务

tasklist 进程列表

schtasks 计划任务

ipconfig /all 判断存在域

net view /domain 判断存在域

net time /domain 判断主域

netstat -ano 当前网络端口开放

nslookup 域名 追踪来源地址

wmic service list brief 查询本机服务

net config workstation 查询当前登录域及登录用户信息

wmic startup get command,caption 查看已启动的程序信息

#架构信息类收集-网络&用户&域控等

net view /domain 查询域列表

net time/domain 从域控查询时间，若当前用户是域用户会从域控返回当前时间，亦用来判 断主域，主域一般用做时间服务器

net localgroup administrators 本机管理员【通常含有域用户】

net user /domain 查询域用户(当前域)

net group /domain 查询域工作组

net group "domain computers" /domain 查看加入域的所有计算机名

net group "domain admins" /domain 查询域管理员用户组和域管用户

net localgroup administrators /domain 查看域管理员

net group "domain controllers" /domain 查看域控

net accounts /domain 查看域密码策略

#关键信息类收集-密码&凭据&口令等

旨在收集各种密文，明文，口令等，为后续横向渗透做好测试准备

计算机用户 HASH，明文获取-mimikatz(win)，mimipenguin(linux)

计算机各种协议服务口令获取-LaZagne(all)，XenArmor(win)，CS 插件

https://github.com/gentilkiwi/mimikatz/

https://github.com/AlessandroZ/LaZagne/

https://github.com/huntergregal/mimipenguin

https://xenarmor.com/allinone-password-recovery-pro-software/

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址