Releases · k8gege/LadonGo

LadonGO 5.2 20231215

Oracle数据库一键提权

5.2 2023.12.14
[+]OracleCmd Oracle远程提权执行操作系统命令
[+]龙芯架构64位 支持的linux kernel版本最低也是5.19,旧版龙芯不支持

基于GO 1.20 一些老旧系统如win2003/xp、unix、liunx低版本不支持
GO 1.20最后一个支持Win7/2008的版本 GO 1.21编译 Win7无法使用

5.2 2023.12.13
[+]OracleSql 执行SQL语句 内置命令ver priv dba
[+]OracleScan Oracle密码爆破 驱动更新为go-ora
[u]OracleScan 支持传统字典user.txt pass.txt爆破
[u]OracleScan 支持sid.txt user.txt pass.txt爆破(sid为数据库名，如orcl)
[u]OracleScan 支持用户密码组合 userpass.txt爆破

LadonGO 5.0 20231208

5.0 2023.12.08
[+]LotusAdmin 检测用户是否Lotus管理员
[u]修复4.9 InfoScan等模块 扫描不了的Bug

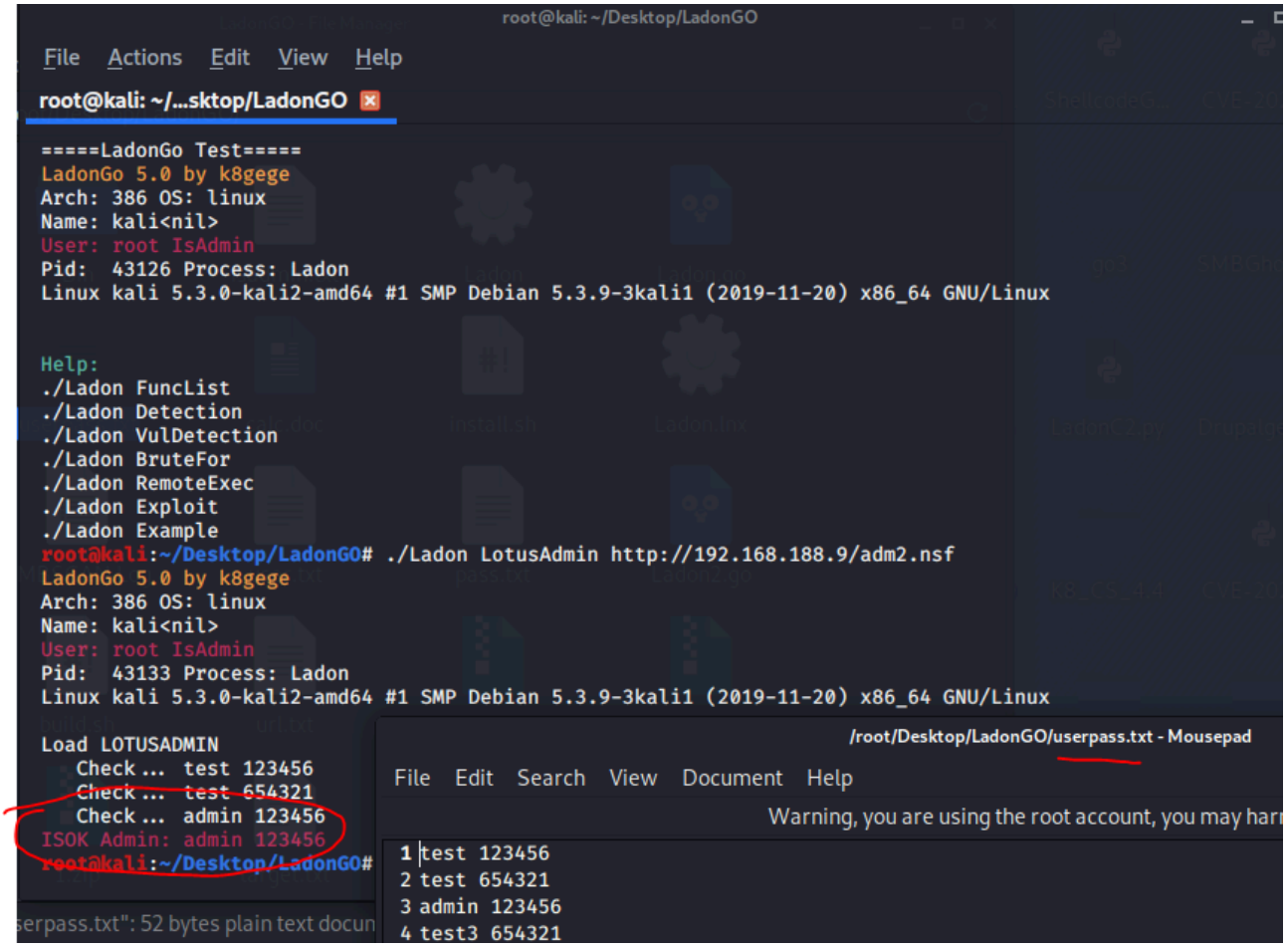
4.9 2023.12.05
[+]HtaSer Hta服务器(不限后缀,如访问doc执行hta)

4.8 2023.1107
[+]InfoScan 一键多协议探测信息
[+]ConfVer ConfluenceVer探测Confluence版本

4.7 20231102
[+]RdpInfo RDP NTLM探测OS信息
[+]HttpInfo HTTP NTLM探测OS信息
[+]HttpsInfo HTTPS NTLM探测OS信息
[+]SmtpInfo HTTP NTLM探测OS信息

4.6 6.28
[+]WmiExec Hash传递执行命令无回显 GO 13.8

[u]修复WinrmCmd SshCmd在4.5更新的问题



LadonGO 4.9 20231205

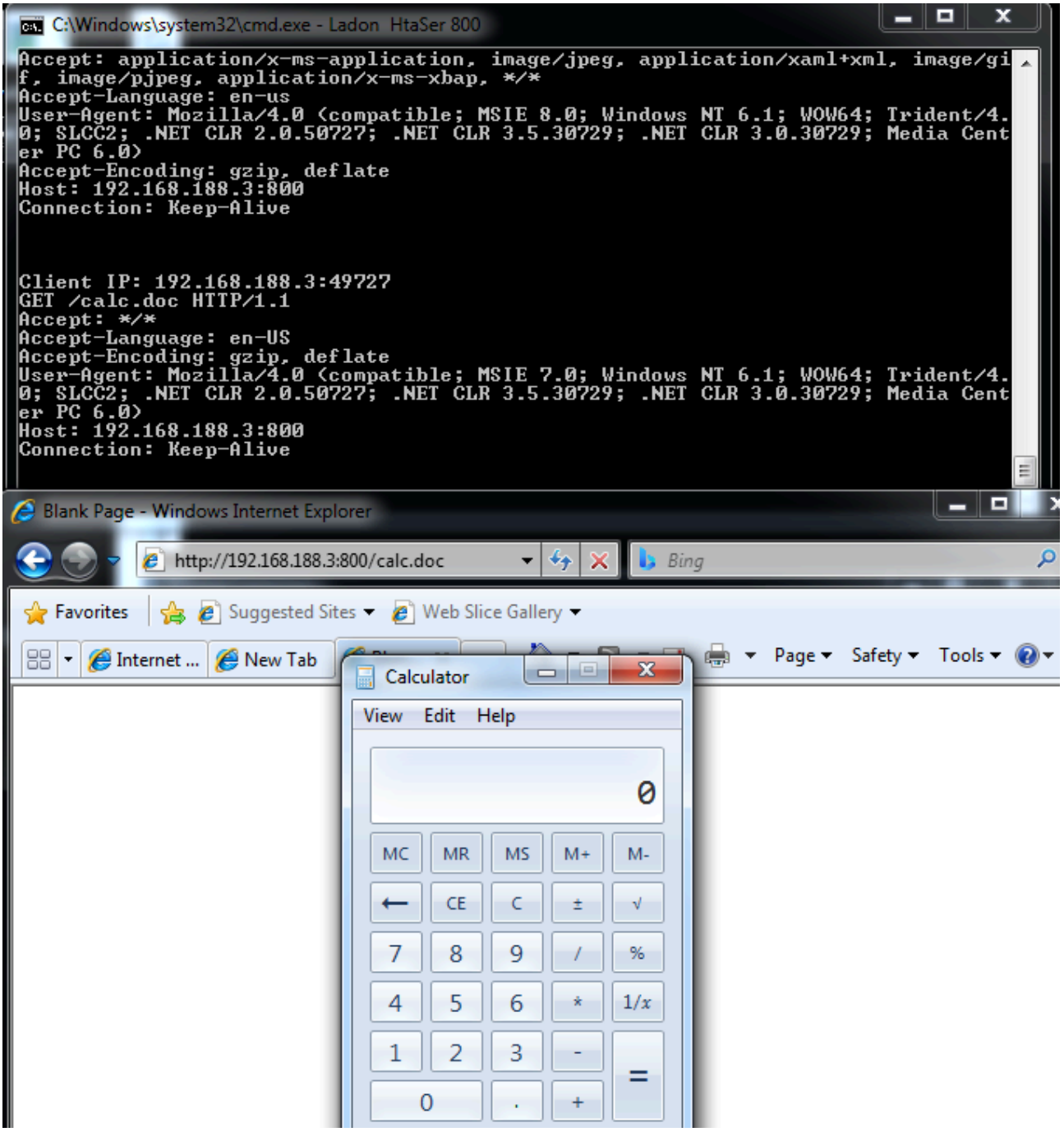
Ladon for Kali/Ubuntu/Mac/Centos/Router/MIPS/ARM

HTA服务器 一键启动 访问DOC也能执行HTA

Ladon和LadonGO用法一致 不限制后缀 访问doc也能执行hta

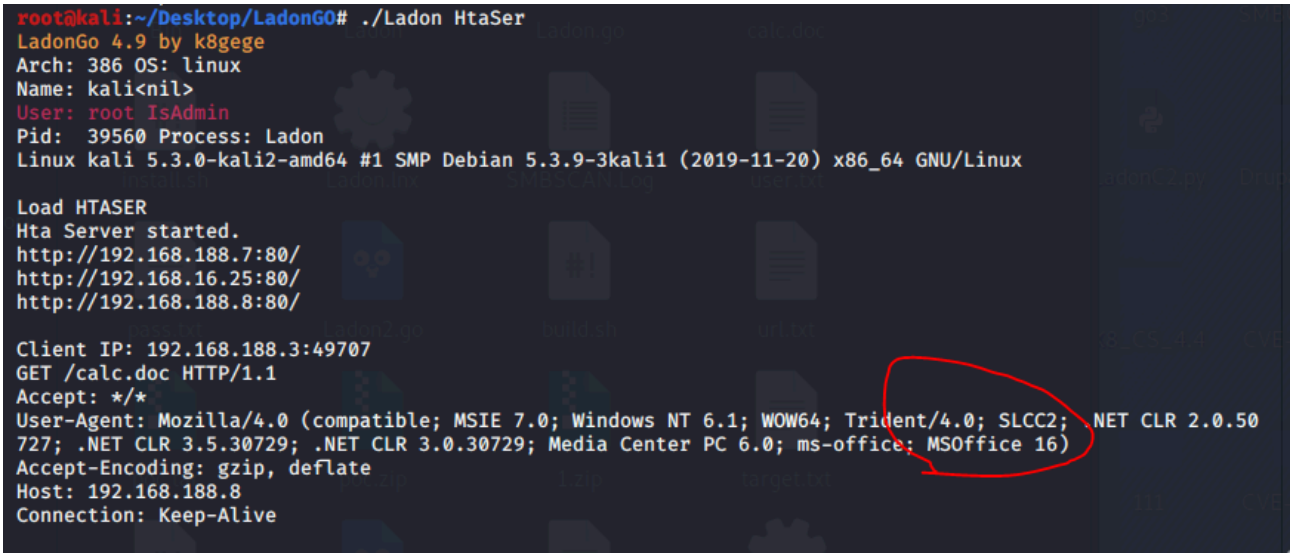
Ladon命令

```
Ladon HtaSer
Ladon HtaSer 8080
```



Kali启动

```
./Ladon HtaSer
./Ladon HtaSer 8080
```



HtaSer.exe

LadonGO 4.8 20231107

4.8 2023.1107

[+]InfoScan 一键多协议探测信息

```
Ladon ip.txt InfoScan
Ladon 192.168.1.8 InfoScan
Ladon 192.168.1.8/24 InfoScan
```

[+]ConfVer ConfluenceVer探测Confluence版本

```
Ladon url.txt ConfVer
Ladon url.txt ConfluenceVer
Ladon ip.txt ConfVer
Ladon 192.168.1.8 ConfVer
Ladon http://192.168.1.8:8090 ConfVer
```

LadonGO 4.7 20231102

4.7 20231102

[+]RdpInfo RDP NTLM探测OS信息

```
root@kali:~/Desktop/LadonGO# ./Ladon rdp://4[redacted]91 RdpInfo
LadonGo 4.7 by k8gege
Arch: 386 OS: linux
Name: kali<nil>
User: root IsAdmin
Pid:  81114 Process: Ladon
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64 GNU/Linux

Targe: rdp://4[redacted]91

ScanStart: 2023-11-02 02:58:03
Load RdpInfo
Target:[redacted]:3389
+------------------+-----------------------------------------------+
|       Server Name | 10_0_8_15                                     |
|       Domain Name | 10_0_8_15                                     |
|       Server FQDN | 10_0_8_15                                     |
|       Domain FQDN | 10_0_8_15                                     |
|     Parent Domain |                                               |
|        OS Ver Num | 6.3.9600                                      |
|        OS Version | Windows 8.1/Server 2012 R2 (Build 9600)       |
+------------------+-----------------------------------------------+
 Finished: 2023-11-02 02:58:03
root@kali:~/Desktop/LadonGO# ./Ladon 43.[redacted]/24 RdpInfo
```

[+]HttpInfo HTTP NTLM探测OS信息

[+]HttpsInfo HTTPS NTLM探测OS信息

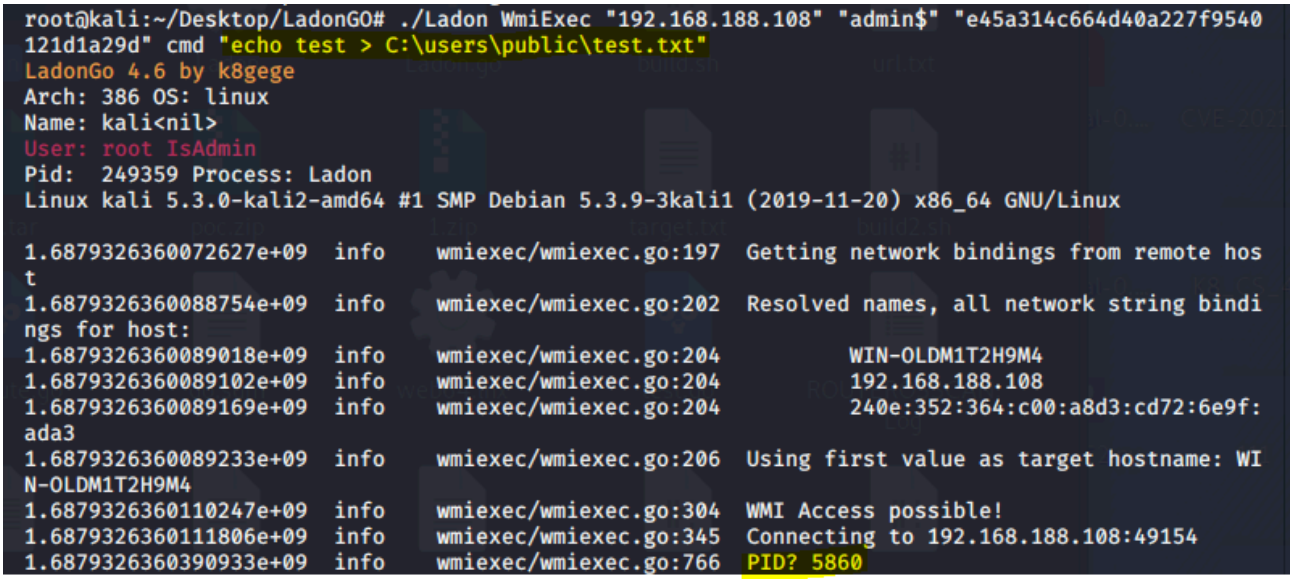
[+]SmtpInfo HTTP NTLM探测OS信息

```
root@kali:~/Desktop/LadonGO# go run ./Ladon.go 205[redacted]2/24 HttpInfo
LadonGo 4.7 by k8gege
Arch: amd64 OS: linux
Name: kali<nil>
User: root IsAdmin
Pid:  81283 Process: Ladon
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64 GNU/Linux

Targe: 205.234.35.52/24

ScanStart: 2023-11-02 03:02:06
Load HttpInfo
Target: http://20[redacted]52
+------------------+-----------------------------------------------+
|       Server Name | SHAREPOINT                                    |
|       Domain Name | [redacted]                                    |
|       Server FQDN | SharePoint.[redacted]a                        |
|       Domain FQDN | t[redacted]                                   |
|     Parent Domain | t[redacted]ca                                 |
|        OS Ver Num | 6.1.7601                                      |
|        OS Version | Windows 7/Server 2008 R2 (Build 7601)         |
+------------------+-----------------------------------------------+
```

4.6 6.28

[+]WmiExec Hash传递执行命令无回显 GO 13.8

[u]修复WinrmCmd SshCmd在4.5更新的问题



LadonGO 4.5 20230618

4.5 6.13

[+]PostShell一句话客户端 支持cmd b64cmd

6.13 修复PortScan不支持自定义端口的BUG

Load PORTSCAN

Ladon 192.168.1.8/24 PortScan

Ladon 192.168.1.8/24 PortScan 21,80,445,443

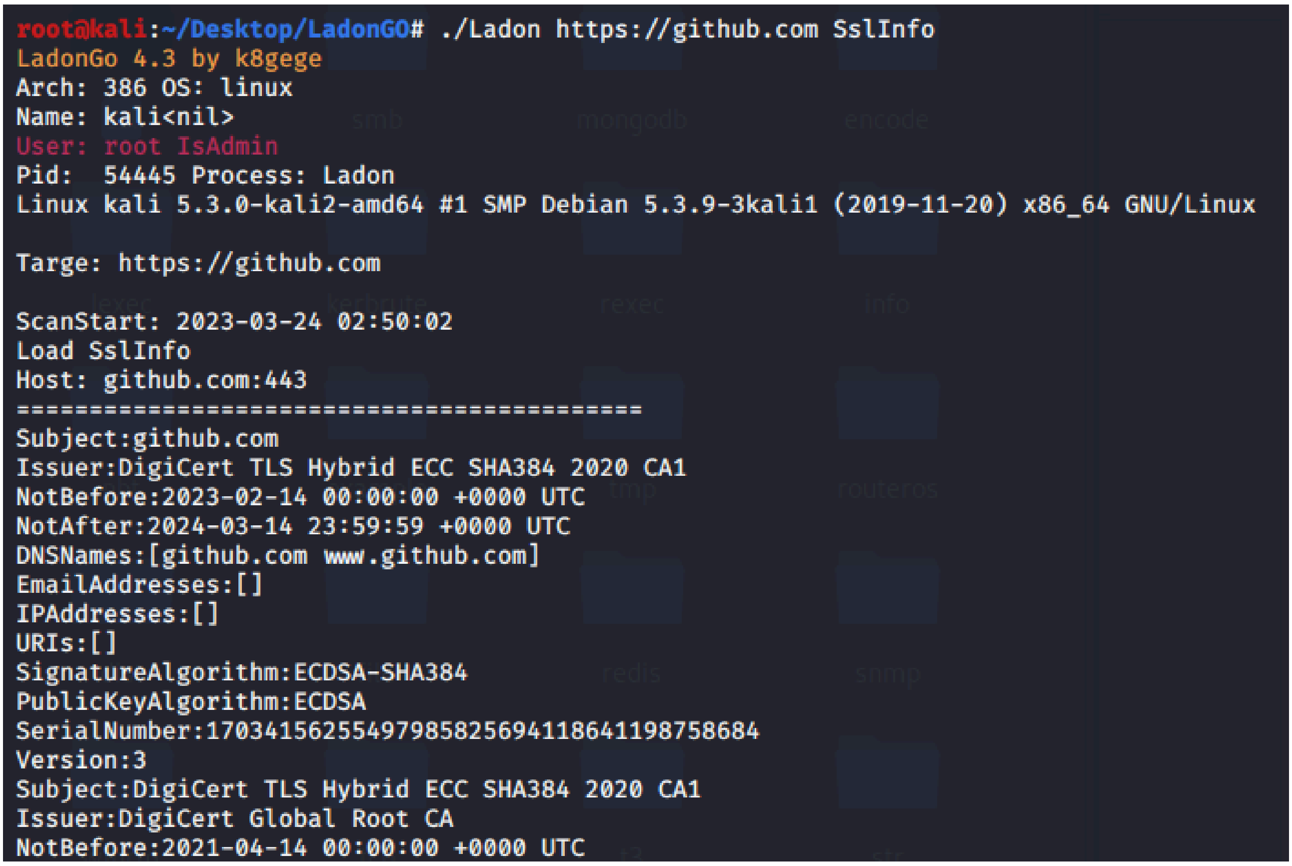
Ladon 192.168.1.8/24 PortScan 21-81

4.4 6.8

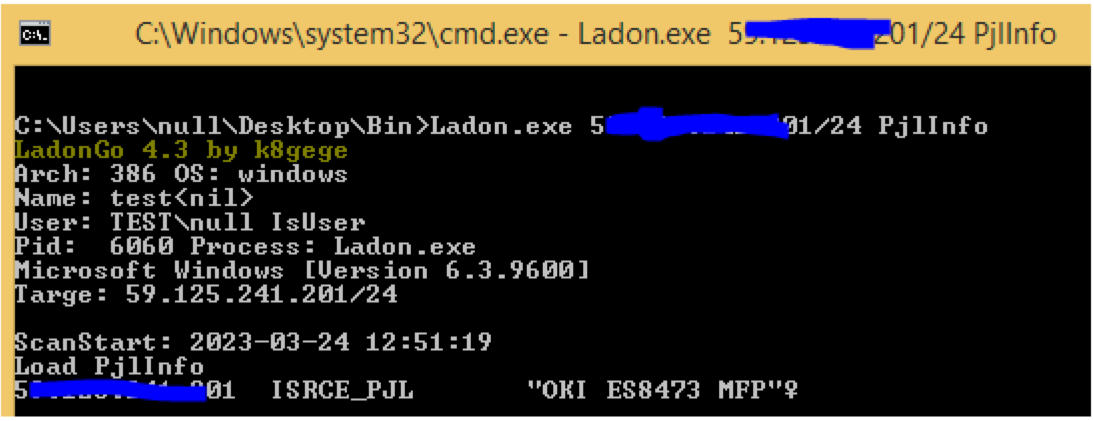
PhpShell 修复有些PHP环境连不了shell的bug

LadonGO 4.3 20230325

SSL证书信息查看CDN、网络设备、防火墙、路由器信息



探测打印机版本 PJL代码执行漏洞检测



LadonGo 4.2 20220728

LadonGo 4.0 20220520

正向Sosck5代理

应用场景

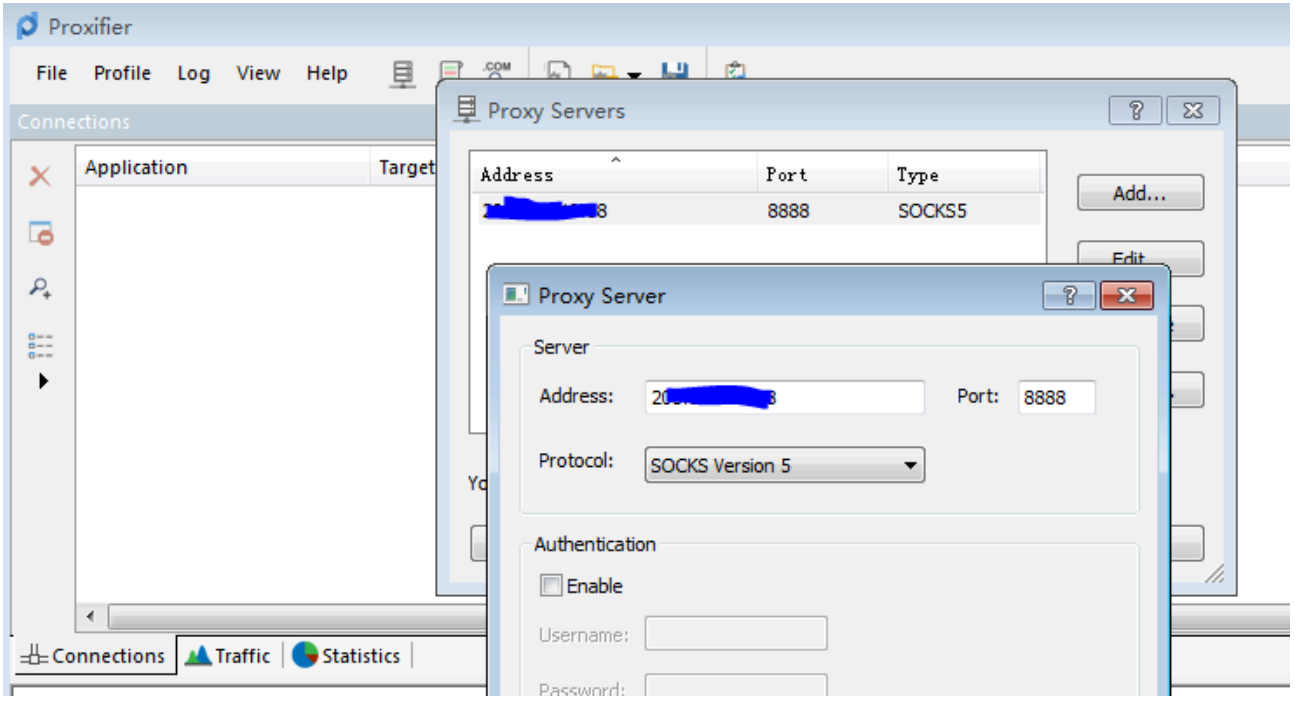
1.自己VPS可上网，开启代理本地上Google查资料
2.目标不可上网(如web服务器)，能上网的更可以
3.路由器系统不含Socks5代理或者开启比较麻烦

执行以下命令开启socks5

Ladon Socks5 ip port

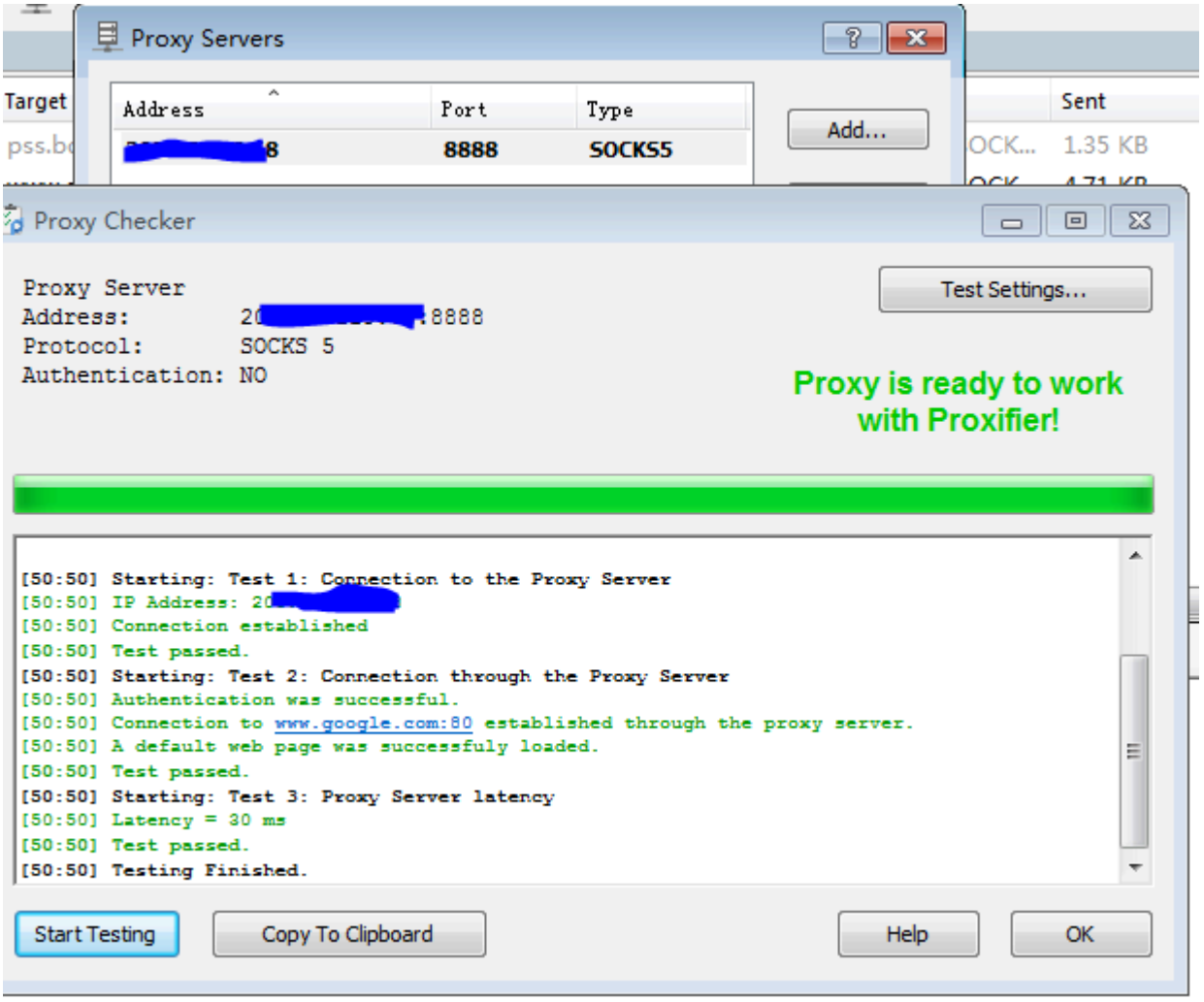
```
=====LadonGo Test=====
LadonGo 4.0 by k8gege
Arch: 386 OS: linux
Name: kali<nil>
User: root IsAdmin
Pid:  113614 Process: Ladon
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64 GNU/Linux

Help:
./Ladon FuncList
./Ladon Detection
./Ladon VulDetection
./Ladon BruteFor
./Ladon RemoteExec
./Ladon Exploit
./Ladon Example
root@kali:~/Desktop/LadonGO# ./Ladon socks5 192.1[redacted] 8888
LadonGo 4.0 by k8gege
Arch: 386 OS: linux
Name: kali<nil>
User: root IsAdmin
Pid:  113699 Process: Ladon
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64 GNU/Linux

Load SOCKS5
Socks5 Starting ...
Listen: 192.1[redacted] 8888
```

连接代理服务器



测试

如果是自己的VPS或目标可上网机器开代理，可以测试是否能上GOOGLE，如果目标不可上网，开启SOCKS代理，就测试是否可访问目标内网而不是用默认的google测试是否代理成功，因为本工具的目的就是为了代理进入内网。



LadonGo 3.9 20220422

Source: https://github.com/k8gege/LadonGo/releases