

# OSCP 筆記

## 起手式

```
scan
ip
port
service
列舉
版本 : CVE
設定
狀態
initial access
interactive shell
PE(提權)
設定
漏洞
套件 package / application
KE ( kernel exploit )
橫移
protocol
ssh
smb
rpc
winRM
```

## 被動資訊

```
憑證
email -> 帳號
域名 -> 帳號
考試一定是自簽(工具忽略警告訊息)

廣度優先
避免兔子坑
```

## portscan

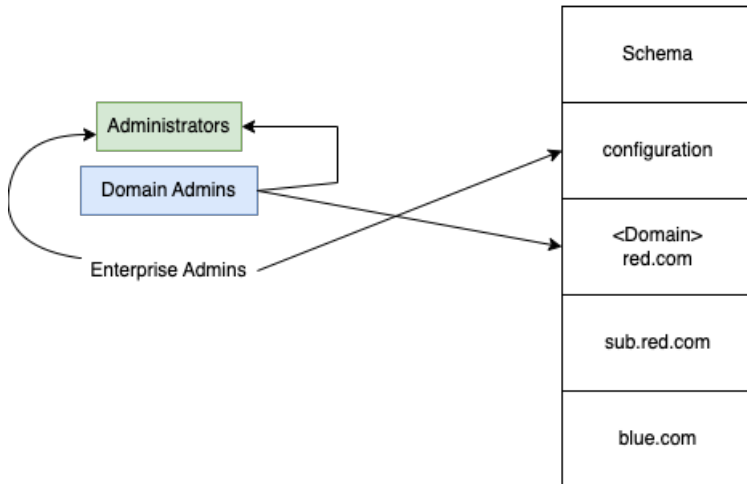
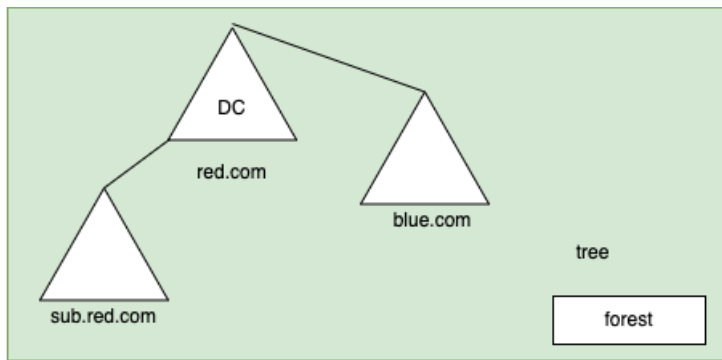
```
portscan
udp icmp type:3,code:3 => 代表沒開

sudo + nmap =>多 ICMP type:8, type:13
區網 arp scan 準確判斷 IP
```

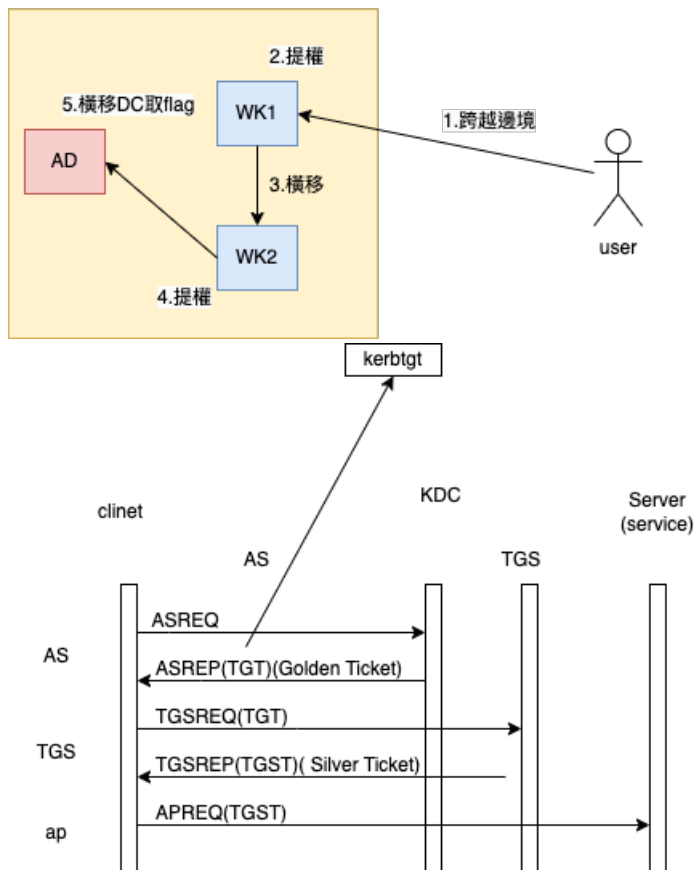
```
# web 攻擊
web -> RCE
E: php, java
sql injection
PT
F1
XSS -> JS

web 進入點
path
from
header
```

## Ch 21



1. 跨越邊境
2. 提權
3. 橫移
4. 提權
5. 橫移DC取flag



PtT  
Ticket Export  
Glden Ticket Attack  
Silver Ticket Attack

## Windows 群組與權限

為了查看權限，我們將使用PowerShell的Get-Acl cmdlet。這個命令本質上將檢索我們使用 -Path 標誌定義的對象的權限並將它們打

印在我們的PowerShell提示中。

```
PS C:\Tools> Get-Acl -Path HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl
```

```
PS C:\Tools> Get-Acl -Path
HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl

Path      :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\LanmanServer\DefaultSecurity\
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Users Allow ReadKey
            BUILTIN\Administrators Allow FullControl
            NT AUTHORITY\SYSTEM Allow FullControl
            CREATOR OWNER Allow FullControl
            APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadKey
            S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-
            3232135806-4053264122-3456934681 Allow ReadKey
```

在清單中突出顯示的輸出顯示了擁有 FullControl 或 ReadKey 權限的組和用戶，這意味著它們都可以讀取 SrvsvcSessionInfo 密鑰本身。

GenericAll: Full permissions on object  
GenericWrite: Edit certain attributes on the object  
WriteOwner: Change ownership of the object  
WriteDACL: Edit ACE's applied to object  
AllExtendedRights: Change password, reset password, etc.  
ForceChangePassword: Password change for object  
Self (Self-Membership): Add ourselves to for example a group

## Word press 起手式

- wp-admin
- readme.html
- wp-login.php

```
# wp 攻擊路徑
WP -> admin -> RCE
    -> CVE-> Core -> RCE
        Theme
        plugin

wp-admin -> DB -> config <- DT
```

## 嘗試登入

```
smvclient -L {ip} -U {password} -> 失敗
crackmapexec smb {ip} -u {username} -p {password} -> 成功
#因為 username 是 網域帳號
```

## Invoke-Ping Invoke-Parallel

🕒 修訂版本 #19

★ 由 treeman 建立於 29 🕒 Q🕒🕒🕒 2023 11:30:26

✍ 由 treeman 更新於 17 🕒 Q🕒G🕒🕒 2023 14:15:49