【SNMP】onesixtyone

OneSixtyOne（也稱為onesixty1或161）是一個用於 SNMP（Simple Network Management Protocol，簡單網路管理協議）掃描的命令行工具。SNMP是一個網絡管理協議，通常用於監控和管理網絡設備，如路由器、交換機、伺服器等。OneSixtyOne 的主要功能是嘗試從目標設備中獲取SNMP Community String（SNMP社區字串），這是一個用於訪問SNMP信息的密鑰。

以下是一些有關 OneSixtyOne 的重要信息：

1. **SNMP Community String**：SNMP社區字串是一個類似密碼的值，用於訪問和控制支持SNMP的設備。不同的設備可能有不同的SNMP社區字串，通常有“讀取（Read）”社區和“寫入（Write）”社區，具體取決於設備的設置。
2. **OneSixtyOne 功能**：OneSixtyOne 主要用於字典攻擊，它嘗試使用預定義的社區字符串清單（通常來自字典文件）來訪問目標設備的SNMP服務。一旦成功找到有效的社區字符串，攻擊者就可以訪問SNMP數據，包括設備配置、性能信息等。
3. **用途**：OneSixtyOne通常用於安全測試、網絡測試或管理目的。系統管理員和安全專業人員可以使用它來確保他們的設備的SNMP設置是安全的，並且未使用弱密鑰。
4. **使用方式**：要使用 OneSixtyOne，你需要提供目標設備的IP地址，並選擇要使用的社區字符串字典文件。然後，OneSixtyOne將嘗試每個社區字符串，看是否可以成功訪問目標設備的SNMP服務。

使用類似onesixtyone的工具，該工具將對一組IP地址進行暴力攻擊。首先，我們需要建立包含社區字符串和我們希望掃描的IP地址的文本文件。這些文件可以幫助我們進行SNMP暴力攻擊。

```
echo public > community
echo private >> community
echo manager >> community
for ip in $(seq 1 254); do echo 192.168.50.$ip; done > ips
onesixtyone -c community -i ips
```

```
onesixtyone 0.3.3 [選項] <主機> <社群>
  -c <社群檔案> 包含嘗試的社群名稱的檔案
  -i <輸入檔案> 包含目標主機的檔案
  -o <輸出檔案> 輸出日誌
  -p 指定替代的目的地SNMP埠口
  -d 調試模式，使用兩次以獲得更多信息

  -s 簡短模式，僅列印IP地址

  -w n 在發送封包之間等待n毫秒（1/1000秒）（默認值為10）
  -q 安靜模式，不要將日誌輸出到標準輸出，與 -o 一同使用
主機可以是IPv4地址或IPv4地址和子網遮罩
默認社群名稱為: public private

最大主機數: 65536
最大社群長度: 32
最大社群數量: 16384

示例: onesixtyone 192.168.4.0/24 public
        onesixtyone -c dict.txt -i hosts -o my.log -w 100
```

⏲修訂版本 #2
★由 treeman 建立於 6 ﷺ 2023 10:27:45
✎由 treeman 更新於 7 ﷺ 2024 19:30:26