

【SNMP】snmpwalk

我們可以使用像snmpwalk這樣的工具來探測並查詢SNMP值，前提是我們知道SNMP的只讀社區字符串，而在大多數情況下它是“public”。

1.3.6.1.2.1.25.1.6.0	System Processes
1.3.6.1.2.1.25.4.2.1.2	Running Programs
1.3.6.1.2.1.25.4.2.1.4	Processes Path
1.3.6.1.2.1.25.2.3.1.4	Storage Units
1.3.6.1.2.1.25.6.3.1.2	Software Name
1.3.6.1.4.1.77.1.2.25	User Accounts
1.3.6.1.2.1.6.13.1.3	TCP Local Ports

使用表1中提供的一些MIB值，我們可以嘗試枚舉它們對應的值。讓我們嘗試對實驗室中已知具有以“public”作為社區字符串的Windows SNMP端口的機器執行以下示例命令。此命令使用-c選項指定社區字符串，-v指定SNMP版本號，以及-t 10選項來增加超時時間到10秒：

```
kali@kali:~$ snmpwalk -c public -v1 -t 10 192.168.50.151
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (78235) 0:13:02.35
iso.3.6.1.2.1.1.4.0 = STRING: "admin@megacorpstwo.com"
iso.3.6.1.2.1.1.5.0 = STRING: "dc01.megacorpstwo.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.2.1.0 = INTEGER: 24
...
```

進一步展示，我們可以使用上面的輸出來獲取目標的電子郵件地址。這些信息可以用來製作針對新發現的聯絡人的社交工程攻擊。

為了進一步練習我們所學的，讓我們探討一些針對Windows目標的SNMP列舉技巧。我們將使用snmpwalk命令，它可以解析MIB Tree的特定分支，稱為OID。

以下示例列舉了dc01機器上的Windows用

```
kali@kali:~$ snmpwalk -c public -v1 192.168.50.151 1.3.6.1.4.1.77.1.2.25
iso.3.6.1.4.1.77.1.2.25.1.1.5.71.117.101.115.116 = STRING: "Guest"
iso.3.6.1.4.1.77.1.2.25.1.1.6.107.114.98.116.103.116 = STRING: "krbtgt"
iso.3.6.1.4.1.77.1.2.25.1.1.7.115.116.117.100.101.110.116 = STRING: "student"
iso.3.6.1.4.1.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.116.111.114 = STRING: "Administrator"
```

我們的命令查詢了與所有本地用戶帳戶名相對應的特定MIB子樹。

作為另一個示例，我們可以列舉所有當前運行的進程：

```
kali@kali:~$ snmpwalk -c public -v1 192.168.50.151 1.3.6.1.2.1.25.4.2.1.2
iso.3.6.1.2.1.25.4.2.1.2.1 = STRING: "System Idle Process"
iso.3.6.1.2.1.25.4.2.1.2.4 = STRING: "System"
iso.3.6.1.2.1.25.4.2.1.2.88 = STRING: "Registry"
iso.3.6.1.2.1.25.4.2.1.2.260 = STRING: "smss.exe"
iso.3.6.1.2.1.25.4.2.1.2.316 = STRING: "svchost.exe"
iso.3.6.1.2.1.25.4.2.1.2.372 = STRING: "csrss.exe"
iso.3.6.1.2.1.25.4.2.1.2.472 = STRING: "svchost.exe"
iso.3.6.1.2.1.25.4.2.1.2.476 = STRING: "wininit.exe"
iso.3.6.1.2.1.25.4.2.1.2.484 = STRING: "csrss.exe"
iso.3.6.1.2.1.25.4.2.1.2.540 = STRING: "winlogon.exe"
iso.3.6.1.2.1.25.4.2.1.2.616 = STRING: "services.exe"
iso.3.6.1.2.1.25.4.2.1.2.632 = STRING: "lsass.exe"
iso.3.6.1.2.1.25.4.2.1.2.680 = STRING: "svchost.exe"
...
```

這個命令返回了一個包含運行進程名稱的字符串數組。這些信息可能非常有價值，因為它可能會顯示存在漏洞的應用程序，或者甚至表明

目標上運行著哪種類型的防病毒軟件。

同樣，我們可以查詢安裝在計算機上的**所有軟件**：

```
kali@kali:~$ snmpwalk -c public -v1 192.168.50.151 1.3.6.1.2.1.25.6.3.1.2
iso.3.6.1.2.1.25.6.3.1.2.1 = STRING: "Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.27.29016"
iso.3.6.1.2.1.25.6.3.1.2.2 = STRING: "VMware Tools"
iso.3.6.1.2.1.25.6.3.1.2.3 = STRING: "Microsoft Visual C++ 2019 X64 Additional Runtime - 14.27.29016"
iso.3.6.1.2.1.25.6.3.1.2.4 = STRING: "Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.27.290"
iso.3.6.1.2.1.25.6.3.1.2.5 = STRING: "Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.27.290"
iso.3.6.1.2.1.25.6.3.1.2.6 = STRING: "Microsoft Visual C++ 2019 X86 Additional Runtime - 14.27.29016"
iso.3.6.1.2.1.25.6.3.1.2.7 = STRING: "Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.27.29016"
...
```

當與我們之前獲得的運行進程列表結合在一起時，這些信息對於交叉檢查目標主機上進程運行的確切軟件版本可以變得非常有價值。

另一種 SNMP 枚舉技術是列出所有當前的**TCP 監聽端口**：

```
kali@kali:~$ snmpwalk -c public -v1 192.168.50.151 1.3.6.1.2.1.6.13.1.3
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.88.0.0.0.0 = INTEGER: 88
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.135.0.0.0.0 = INTEGER: 135
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.389.0.0.0.0 = INTEGER: 389
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.445.0.0.0.0 = INTEGER: 445
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.464.0.0.0.0 = INTEGER: 464
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.593.0.0.0.0 = INTEGER: 593
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.636.0.0.0.0 = INTEGER: 636
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.3268.0.0.0.0 = INTEGER: 3268
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.3269.0.0.0.0 = INTEGER: 3269
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.5357.0.0.0.0 = INTEGER: 5357
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.5985.0.0.0.0 = INTEGER: 5985
...
```

加上-Oa 可以解碼16進制資料

```
$ snmpwalk -c public -v1 -t 10 192.168.202.151
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 25 Model 1 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (492426016) 56 days, 23:51:00.16
iso.3.6.1.2.1.1.4.0 = STRING: "admin@megacorpstwo.com"
iso.3.6.1.2.1.1.5.0 = STRING: "dc01.megacorpstwo.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.2.1.0 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
...
iso.3.6.1.2.1.2.2.1.1.22 = INTEGER: 22
iso.3.6.1.2.1.2.2.1.1.23 = INTEGER: 23
iso.3.6.1.2.1.2.2.1.1.24 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 53 6F 66 74 77 61 72 65 20 4C 6F 6F 70 62 61 63
6B 20 49 6E 74 65 72 66 61 63 65 20 31 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 36 74 6F 34 20 41
64 61 70 74 65 72 00
```

```
$ snmpwalk -c public -v1 -t 10 192.168.202.151 -Oa
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 25 Model 1 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (492428968) 56 days, 23:51:29.68
iso.3.6.1.2.1.1.4.0 = STRING: "admin@megacorpstwo.com"
iso.3.6.1.2.1.1.5.0 = STRING: "dc01.megacorpstwo.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.2.1.0 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
```

...

iso.3.6.1.2.1.2.2.1.1.21 = INTEGER: 21

iso.3.6.1.2.1.2.2.1.1.22 = INTEGER: 22

iso.3.6.1.2.1.2.2.1.1.23 = INTEGER: 23

iso.3.6.1.2.1.2.2.1.1.24 = INTEGER: 24

iso.3.6.1.2.1.2.2.1.2.1 = STRING: "Software Loopback Interface 1."

iso.3.6.1.2.1.2.2.1.2.2 = STRING: "Microsoft 6to4 Adapter."

iso.3.6.1.2.1.2.2.1.2.3 = STRING: "WAN Miniport (PPTP)."

iso.3.6.1.2.1.2.2.1.2.4 = STRING: "WAN Miniport (GRE)."

🕒修訂版本 #2

★由 treeman 建立於 6 🕒🕒@🕒🕒 2023 10:38:30

✍由 treeman 更新於 7 🕒@🕒🕒 2024 19:30:26