Enumerando SNMP

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SNMP - Porta 161 - UDP
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

→ Simple Network Management Protocol

+ Protocolo para gerenciamento de dispositivos na rede

IMPORTANTE	
SNMP	161 (UDP)
OID - Object Identifier	Código utilizado para identificar os objetos
MIB - Management Information Base	Base contendo informações relacionadas ao gerenciamento de redes
Community	Valor utilizado entre as partes snmp para troca de informações

Nível de acesso (Community)
RO – Read Only – Acesso de leitura
RW – Read Write – Acesso de leitura / escrita

EXEMPLOS

VALORES MIBS	
1.3.6.1.2.1.25.1.6.0	PROCESSOS DO SISTEMA
1.3.6.1.4.1.77.1.2.25	CONTAS DE USUÁRIOS
1.3.6.1.2.1.6.13.1.3	PORTAS TCP

https://www.alvestrand.no/objectid/1.3.6.1.2.1.html
http://www.oid-info.com/

COMMUNITY	
public	manager
private	access
cisco	secret

→ é bom ler o manual do fabricante

+ Buscando pelos hosts que usam esse protocolo:

```
nmap -sVU -p 161 -Pn <endereço de ip>
```

→ lembrando que o snmp funciona no protocolo udp

+ Uma outra alternativa é o onesixtyone
→ ele pode ajudar a fazer uma varredura pelas communities liberadas, mas para isso, devemos carregá-las em uma lista txt

```
onesixtyone -c comu.txt 172.16.1.0/24
```

+ A partir das info coletadas anteriormente, devemos agora partir para a enumeração com as MIB's apropriadas (que podem ser cosultadas nos sites acima)

```
root@pentest:~/Desktop# snmpwalk -c public -v1 172.16.1.4 1.3.6.1.4.1.77.1.2.25
iso.3.6.1.4.1.77.1.2.25.1.1.7.85.115.117.97.114.105.111 = STRING: "Usuario"
iso.3.6.1.4.1.77.1.2.25.1.1.7.114.97.102.97.101.108.97 = STRING: "rafaela"
iso.3.6.1.4.1.77.1.2.25.1.1.9.67.111.110.118.105.100.97.100.111 = STRING: "Convidado"
iso.3.6.1.4.1.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.100.111.114 = STRING: "Administrador"
iso.3.6.1.4.1.77.1.2.25.1.1.13.72.101.108.112.65.115.115.105.115.116.97.110.116 = STRING: "HelpAssistant"
iso.3.6.1.4.1.77.1.2.25.1.1.15.75.69.89.50.57.56.55.48.48.49.57.49.56.50.48 = STRING: "KEY298700191820"
iso.3.6.1.4.1.77.1.2.25.1.1.16.83.85.80.80.79.82.84.95.51.56.56.57.52.53.97.48 = STRING: "SUPPORT_388945a0"
```

→ Com o comando snmpwalk, pudemos usar a community (-c)apropriada, que foi descoberta outrora, e passar a MIB que faz a varredura dos usuários

+ Caso quiséssemos passar todas as MIB's, basta que executemos:

`snmpwalk -c public -v1 172.16.1.4` → basta n passar a MIB

+ Para que a saída fique mais legível, devemos instalar o snmp-mibs-downloader no kali

+ Para validar o uso dessa aplicação, basta executarmos

`echo "" > etc/snmp/snmp.conf`

→ agora podemos executar novamente o comando snmpwalk citado acima que a saída já vai estar mais limpa

+ Agora podemos pesquisar pelas MIB's usando nomes, n mais números

`snmptranslate -IR sysUpTime`

→ pesquisa pelas mibs mais próximas dessa sysuptime
→ agora, em vez de digitarmos o numero da mib, digitamos seu delicioso nome

+ Para ver detalhes sobre alguma consulta que estejamos fazendo, basta

`snmptranslate -Td <mib>`

+ Para pesquisar:

`snmptranslate -TB icmp`