Network Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Pentesting Routers: SNMP audit Braa and Nmap NSE Scripts

Braa SNMP Walk

```
PentesterAcademy# braa a1d2@192.168.1.101:161:.1.3.6.1.*
192.168.1.101:20ms:.1.3.6.1.2.1.1.1.0:Vyatta VC6.6R1
192.168.1.101:20ms:.1.3.6.1.2.1.1.2.0:.1.3.6.1.4.1.30803
192.168.1.101:20ms:.1.3.6.1.2.1.1.3.0:177123
192.168.1.101:21ms:.1.3.6.1.2.1.1.4.0:root
192.168.1.101:20ms:.1.3.6.1.2.1.1.5.0:vyatta
192.168.1.101:22ms:.1.3.6.1.2.1.1.6.0:Unknown
192.168.1.101:20ms:.1.3.6.1.2.1.1.7.0:14
192.168.1.101:21ms:.1.3.6.1.2.1.1.8.0:5
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.2.1:.1.3.6.1.2.1.10.131
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.2.2:.1.3.6.1.6.3.11.3.1.1
192.168.1.101:22ms:.1.3.6.1.2.1.1.9.1.2.3:.1.3.6.1.6.3.15.2.1.1
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.2.4:.1.3.6.1.6.3.10.3.1.1
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.2.5:.1.3.6.1.6.3.1
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.2.6:.1.3.6.1.2.1.49
192.168.1.101:126020ms:.1.3.6.1.2.1.1.9.1.2.7:.1.3.6.1.2.1.4
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.2.8:.1.3.6.1.2.1.50
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.2.9:.1.3.6.1.6.3.16.2.2.1
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.2.10:.1.3.6.1.6.3.13.3.1.3
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.2.11:.1.3.6.1.2.1.92
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.1:RFC 2667 TUNNEL-MIB implementation for Linux 2.2.x kernels.
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.2:The MIB for Message Processing and Dispatching.
192.168.1.101:22ms:.1.3.6.1.2.1.1.9.1.3.3:The management information definitions for the SNMP User-based
Security Model.
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.4:The SNMP Management Architecture MIB.
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.3.5:The MIB module for SNMPv2 entities
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.6:The MIB module for managing TCP implementations
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.7:The MIB module for managing IP and ICMP implementations
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.3.8:The MIB module for managing UDP implementations
192.168.1.101:21ms:.1.3.6.1.2.1.1.9.1.3.9:View-based Access Control Model for SNMP.
192.168.1.101:20ms:.1.3.6.1.2.1.1.9.1.3.10:The MIB modules for managing SNMP Notification, plus filtering
```

Braa SNMP SET

Try On your own ☺

Nmap

File `snmp-brute`

Script types: portrule
Categories: ***intrusive***, ***brute***
Download: **http://nmap.org/svn/scripts/snmp-brute.nse**

User Summary

Attempts to find an SNMP community string by brute force guessing.

This script opens a sending socket and a sniffing pcap socket in parallel threads. The sending socket sends the SNMP probes with the community strings, while the pcap socket sniff probes. If valid community strings are found, they are added to the creds database and reported in the output.

The script takes the `snmp-brute.communitiesdb` argument that allows the user to define the file that contains the community strings to be used. If not defined, the default wordli community strings is `nselib/data/snmpcommunities.lst`. In case this wordlist does not exist, the script falls back to `nselib/data/passwords.lst`

No output is reported if no valid account is found.

Script Arguments

snmp-brute.communitiesdb

The filename of a list of community strings to try.

passdb, unpwdb.passlimit, unpwdb.timelimit, unpwdb.userlimit, userdb

See the documentation for the **unpwdb** library.

snmpcommunity

See the documentation for the **snmp** library.

Example Usage

```
nmap -sU --script snmp-brute <target> [--script-args snmp-brute.communitiesdb=<wordlist> ]
```

Script Output

```
PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|   dragon - Valid credentials
|_  jordan - Valid credentials
```

Nmap snmp-brute

```
PentesterAcademy# nmap -sU -p 161 -n --script snmp-brute 192.168.1.101 --script-args snmp-brute
.communitiesdb=wordlist

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-06 04:17 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00044s latency).
PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|_  a1d2 - Valid credentials
MAC Address: 08:00:27:81:4B:34 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
PentesterAcademy#
```

Nmap snmp-interfaces

File `snmp-interfaces`

Script types: prerule, portrule
Categories: ***default***, ***discovery***, ***safe***
Download: **http://nmap.org/svn/scripts/snmp-interfaces.nse**

User Summary

Attempts to enumerate network interfaces through SNMP.

This script can also be run during Nmap's pre-scanning phase and can attempt to add the SNMP server's interface addresses to the target list. The script argument `snmp-interfaces.host` is required to know what host to probe. To specify a port for the SNMP server other than 161, use `snmp-interfaces.port`. When run in this way, the script's output tells how many new targets were successfully added.

Script Arguments

snmp-interfaces.host

Specifies the SNMP server to probe when running in the "pre-scanning phase".

snmp-interfaces.port

The optional port number corresponding to the host script argument. Defaults to 161.

max-newtargets, newtargets

See the documentation for the **target** library.

snmpcommunity

See the documentation for the **snmp** library.

Example Usage

```
nmap -sV -sC <target>
```

http://nmap.org/nsedoc/scripts/snmp-interfaces.html

Nmap snmp-interfaces

```
PentesterAcademy# nmap -sU -sV -p 161 192.168.1.101 --script="snmp-interfaces"

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-19 22:08 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00055s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    net-snmp
MAC Address: 08:00:27:81:4B:34 (Cadmus Computer Systems)
```

```
PentesterAcademy# nmap -sU -sV -p 161 192.168.1.101 --script="snmp-interfaces" --script-args="snmpc
ommunity=a1d2"

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-19 22:09 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00038s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    net-snmp
| snmp-interfaces:
|   lo
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 10 Mbps
|     Status: up
|     Traffic stats: 98.42 Kb sent, 98.42 Kb received
|   Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
|     IP address: 192.168.1.101  Netmask: 255.255.255.0
|     MAC address: 08:00:27:81:4b:34 (Cadmus Computer Systems)
|     Type: ethernetCsmacd  Speed: 100 Mbps
|     Status: up
|_    Traffic stats: 414.78 Kb sent, 1.22 Mb received
MAC Address: 08:00:27:81:4B:34 (Cadmus Computer Systems)
```

Nmap snmp-netstat

```
PentesterAcademy# nmap -sU -sV -p 161 192.168.1.101 --script="snmp-netstat" --script-args="snmpcomm
unity=a1d2"

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-19 22:10 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00057s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    net-snmp
| snmp-netstat:
|   TCP  0.0.0.0:22          0.0.0.0:0
|   TCP  0.0.0.0:80          0.0.0.0:0
|   TCP  0.0.0.0:443         0.0.0.0:0
|   TCP  127.0.0.1:199       0.0.0.0:0
|   TCP  127.0.0.1:199       127.0.0.1:49285
|   TCP  127.0.0.1:199       127.0.0.1:49286
|   TCP  127.0.0.1:199       127.0.0.1:49287
|   TCP  127.0.0.1:49285     127.0.0.1:199
|   TCP  127.0.0.1:49286     127.0.0.1:199
|   TCP  127.0.0.1:49287     127.0.0.1:199
|   UDP  0.0.0.0:123         *:*
|   UDP  0.0.0.0:161         *:*
|   UDP  127.0.0.1:123       *:*
|_  UDP  192.168.1.101:123   *:*
MAC Address: 08:00:27:81:4B:34 (Cadmus Computer Systems)
```

Nmap snmp-processes

```
PentesterAcademy# nmap -sU -sV -p 161 192.168.1.101 --script="snmp-processes" --script-args="snmpco
mmunity=a1d2"

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-19 22:11 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00042s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    net-snmp
| snmp-processes:
|   init
|     Path: init [2]
|     PID: 1
|   udevd
|     Path: udevd
|     Params: --daemon
|     PID: 1240
|   udevd
|     Path: udevd
|     Params: --daemon
|     PID: 1386
|   udevd
|     Path: udevd
|     Params: --daemon
|     PID: 1418
|   acpid
|     Path: /usr/sbin/acpid
|     PID: 1885
|   atd
|     Path: /usr/sbin/atd
|     PID: 1887
```

Nmap snmp-sysdescr

```
PentesterAcademy# nmap -sU -sV -p 161 192.168.1.101 --script="snmp-sysdescr" --script-args="snmpcom
munity=a1d2"

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-19 22:12 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00043s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    net-snmp
| snmp-sysdescr: Vyatta VC6.6R1
|_  System uptime: 0 days, 0:43:22.45 (260245 timeticks)
MAC Address: 08:00:27:81:4B:34 (Cadmus Computer Systems)
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

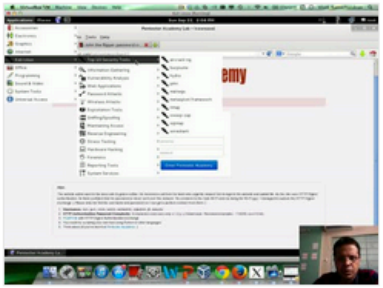
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

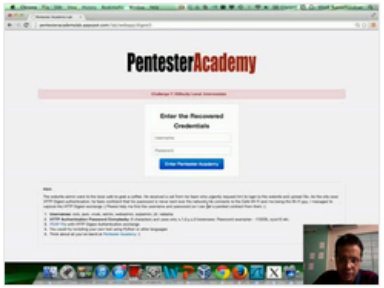
Start Learning Today!

Latest Videos

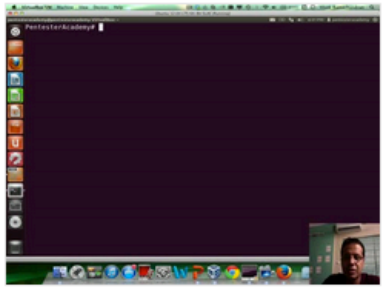
New content added weekly!



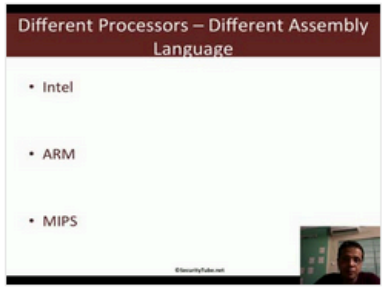
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux