

Playing with SIP, NMAP and NSE, now writing a SIP library...

publié par malphx le lundi, août 23 2010 - 23:54



Since my last post, I finally decided to start writing a SIP library for nmap. This lib will be minimalist and be largely based on the http.lua library taken from Nmap 5.0

It will be used by two NSE scripts:

- sip-extscan.nse: a script which try to list (find) valid SIP extensions on a SIP register
- sip-brute.nse: a script that try to bruteforce SIP extensions password on a register

Here are the first result:

The target used for the test is a Tribbox based host (Asterisk PBX 1.6.0.26-FONCORE-r78)

With actually four extensions:

Actualy 5000 sip extensions, a weak password and use the unpwdb library

```
sudo nmap -sU -p U:5060 -T5 --script
sip-map2,sip-extscan3,sip-brute2 --script-args
exten_range="5000-5010" 172.17.0.53
```

Starting Nmap 5.00 (<http://nmap.org>) at 2010-08-23 23:20 CEST

Interesting ports on 172.17.0.53:

PORT STATE SERVICE

5060/udp open sip

|_ sip-map2: SIP 2.0 device detected

| sip-extscan3:

| Unprotected Extensions

| 5003

| Protected Extensions

| 5000

| 5001

|_ 5002

| sip-brute2:

| exten: 5001 Password: 1234

|_ exten: 5002 Password: 1234

Nmap done: 1 IP address (1 host up) scanned in 107.24 seconds
It seems that the work is in the good way, however, a lot of testing must still be done.

Playing with SIP, NMAP and NSE

publié par malphx le mardi, août 17 2010 - 19:04



In the last [Honeynet Project's Forensic Challenge \(FC4\)](#), one question (Section 1, question 2) caught my attention.

It was about the possibility that the given log file could have been generated using a simple Nmap UDP scan.

In the challenge, the answer was : No.

Because a simple Nmap's UDP scan uses UDP packets without any payload and thus could not generate valid SIP requests.

But, Nmap offers a powerful scripting engine: [Nmap Scripting Engine](#) or NSE.

With NSE it is possible to interact with the targetted host using simple to complex communication exchanges.

After having read the NSE part of the [Nmap book](#), I decided to give a try at NSE.

My first NSE script (modestly) behaves like the [SIPvicious](#) tool: svmap.py.

This script, named sip-map.nse tries to find valid SIP server by sending a SIP OPTIONS request using the UDP protocol.

Usage:

```
# Without version (User-Agent) information
sudo nmap -sU -p U:5060 -script sip-map.nse
# With version information
sudo nmap -sU -p U:5060 -sV -script sip-map.nse
```

Output:

```
Interesting ports on X.X.X.X:
PORT STATE SERVICE VERSION
```

```
5060/udp open sip Asterisk PBX 1.6.0.26-FONCORE-r78  
|_ sip-map: SIP 2.0 compliant device detected
```

sip-map.nse is the first script from a series of scripts I wish to write.
These scripts will be about SIP scanning with a behaviour close to the SIPvicious tools but using Nmap.

You can download it here: [sip-map.nse](#)

Feel free to leave a comment !