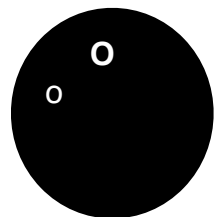




how to get the job done

by sandro gauci



Visit <http://sipvicious.org/> for more information on the tools

The objective was to get the latest research documents from the lab servers. Chris didn't ask why, and they never asked how, but he did not think it would be much of a problem. His previous experience had taught him that no one seems to take these things too seriously until its too late. Especially for someone from the inside. But Pharmakom Industries seemed a bit different. It was the third day since the meeting, his 'research' had been exhaustive and had had no luck yet.

"I **must** be missing something".

Chris was getting frustrated. He recounted all the things he had done by now. He was not using Nessus or anything like that. He wanted to make sure that his actions stay under the radar for a long while. That made using automated tools a big no no. The servers were patched to the latest and his exploits would not have worked anyway. He had scanned the personal computers of the key people who might have access, with hopes to find some vulnerable 3rd party software. He had even launched an on-going password guessing attack on some user's domain account, with slow and random intervals in order to avoid locking out their account. But the password complexity policies seemed to be doing their job quite well. Checked the permissions on the fileserver's shares. All to no avail. If he had more time he would simply wait for a zero day or buy one off ZeroBay. But no chance for that - tomorrow was the deadline and he had better give them some good news!

...

"Well, I guess I need to apply some grey matter on this one". Since he had started doing these kind of odd jobs, Chris had learnt that most of the times they didn't need the brain power that everyone seemed to believe. But this time it was different. As he kept trying to think up of new ways to get the documents, he became aware of what was facing him.

"The phone system! That's the key." The phone had a label with numbers, amongst them the Help Desk Support - extension 123. He decided to give them a call:

"Hi, I think I locked out my account, could you check for me please?"

"Hi Chris, your username is "chr006" right? Everything seems to be fine on this end"

"Let me check .. oh ok works now!"

"Thanks"

That was easy. Now he knew that the support checked for who called, probably by relying on the caller id. They even made sure that the claims are indeed for real. He couldn't just go ahead and call them pretending to be the CEO or just about anyone. He had to get his target to call him instead. He liked to be helpful, especially to people in the upper management.

"Ok things are finally moving", exclaimed Chris as he proceeded to check the make of the phone. It was a Grandstream.

```
C:\sipvicious>svmap.py 10.0.0.1/16 -v
INFO:root:start your engines
INFO:DrinkOrSip:10.0.2.1:5060 -> 10.0.2.1:5060 -> Asterisk PBX
INFO:DrinkOrSip:10.0.2.20:5060 -> 10.0.2.20:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.21:5060 -> 10.0.2.21:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.22:5060 -> 10.0.2.22:5060 -> Grandstream BT100
INFO:DrinkOrSip:10.0.2.23:5060 -> 10.0.2.23:5060 -> Grandstream BT100
WARNING:root:caught your control^c - quitting
INFO:root:we have 5 devices
```

SIP Device	User Agent
10.0.2.1:5060	Asterisk PBX
10.0.2.20:5060	Grandstream BT100 1.0.6.7
10.0.2.20:5060	Grandstream BT100 1.0.6.7
10.0.2.20:5060	Grandstream BT100 1.0.6.7
10.0.2.20:5060	Grandstream BT100 1.0.6.7

```
INFO:root:Total time: 0:00:04.384883
```

Chris then proceeded to use svwar to make sure that the extension works on the Asterisk PBX.

```
C:\sipvicious>svwar.py 10.0.2.1 -e 123 -v
INFO:root:start your engines
INFO:TakeASip:Ok SIP device found
INFO:TakeASip:extension '123' exists - requires authentication
INFO:root:we have 1 extensions
| Extension | Authentication |
-----|-----|
| 123      | reqauth       |

INFO:root:Total time: 0:00:03.115869
```

His next step was to launch a password guessing attack on help desk.

```
C:\sipvicious>svcrack.py 10.0.2.1 -u 123 -d dictionary.txt
INFO:root: scan started at 2021-07-21 13:01:32.23143
INFO:ASipOfRedWine:The password for 123 is vagrant
INFO:root:we have 1 cracked users
| Extension | Password |
-----|-----|
| 123      | vagrant  |

INFO:root:Total time: 0:00:32.145588
```

Aha! He then launched his trusty SIP client and punched in the extension, password and name of the SIP registrar. It was time to test this out. He proceeded to use the Grandstream phone to call the help desk. His X-lite started buzzing. He immediately alt+f4'ed X-lite before any legitimate calls get routed to his IP.

To get someone from the R&D department to call him, he had to do something which would prompt him or her to call the help desk. It was time to make use of the Active Directory.

Launching "Find people or computers" from his Windows box, he punched "research" in the search field, and pressed enter. Whoever set up the entries had been extra helpful, providing information on the roles of each employee that matched the query. Pamela Kellman seemed like a good candidate as victim. She was a supervisor and would have access to the Research and Development directories on the file servers.

```
C:\>net use \\pamela\admin$ "test" /user:pharmakom\pam002
System error 1326 has occurred.
```

Logon failure: unknown user name or bad password.

```
C:\>net use \\pamela\admin$ "test" /user:pharmakom\pam002
System error 1326 has occurred.
```

Logon failure: unknown user name or bad password.

```
C:\>net use \\pamela\admin$ "test" /user:pharmakom\pam002
System error 1909 has occurred.
```

The referenced account is currently locked out and may not be logged on to.

It was time to get the call! Chris started his X-lite soft phone, expecting a phone call anytime soon.

"Hi, my outlook is asking for username and password. Could you fix this for me please?"

"Hi Mrs. Kellman. No problem, could you log out and back in please?"

"Sure let me save everything"

... few seconds later ...

"It's telling me that my account is locked out, just unlock it for me please"

"It doesn't appear to be locked out, but we just had some others experience this. Did your password have any strange characters?"

"Er..."

"Could you give me your password so that I check for you?"

"Sure, it's Joanna underscore nine teen eighty six"

"Hold on the line ma'am"

Chris then put the call on hold and called help desk.

"Hi, I'm gonna forward Pamela Kellman from research, could you just unlock her account please?"

"Sure, no problem!"

Chris waited for what seemed like an eternity and then decided to give it a try. Went back to his command line

```
C:\>net use Z: \\fileserver\departments "joanna_1986" /user:pharmakom\pam002
```

Now he could access to the research folder by accessing Z:\research directly from his machine. He sorted the documents by date modified and grabbed the last three folders. "Guess it would be one of these", he thought and proceeded to compress and encrypt the files with 7-zip. Then he launched Firefox and logged in to his temporary gmail account, created a new email and clicked on "attach a file". Following a click on the "browse" button, he searched for the file he had just encrypted, and finally clicked on save. The documents were now saved in his gmail drafts for later use. Time to go out and party!

...

The phone had been ringing for a while. Chris scrubbed his eyes and grabbed the phone as he looked at the bright red LEDs. It was 9am.

"Uh?" - he didn't feel like answering the phone like normal people do.

"Hi Chris, good morning", was the voice at the other end of the line. It sounded pretty familiar.

"Hi there Mr. Takahashi, I was just about to call you - how are things?"

"Good good - listen, do you think your report will be ready by next Tuesday? How did the Penetration Test go?"

"Very well sir. It will be done by then", he replied, with a broad smile.