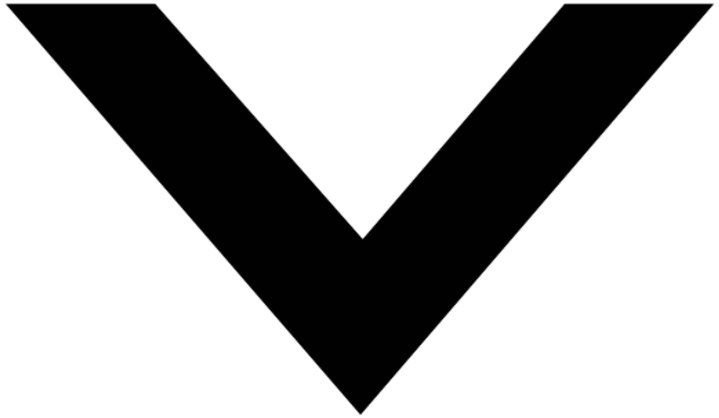


VICXER

SAP Hash Cracking With John The Ripper

Jordan Santarsieri

jsantarsieri@vicxer.com

DISCLAIMER

- This publication contains references to the products of SAP AG. SAP R/3, SAP NetWeaver and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany, US and in several other countries all over the world.

- SAP AG, neither the authors nor the publishers of this publication are responsible for its content and the SAP group shall not be liable for errors / omissions on these materials.

ABOUT US

WE ARE VICXER!

- A company focused in securing the business critical applications and its adjacent infrastructure (SAP, Oracle Siebel and others)
- All of our customers belong to the Fortune-500 Group
- We do:

  Oracle & SAP Penetration Testing

  ERP Cyber-Security Trainings

  Vulnerability Assessment and Management

  SAP Forensics & Many More!

VICXER

JORDAN SANTARSIERI

VICXER'S FOUNDER

Originally devoted to Penetration Testing, Vulnerability Research & Exploit writing, discovered several vulnerabilities in Oracle, SAP, IBM and many others.

Speaker and trainer at Black-Hat, OWASP-US, Hacker Halted, Ekoparty, etc.
I started researching ERP Software back in **2008!**

Had the honor to secure more than **1000 SAP implementations** all around the globe, including Fortune-500 companies, military institutions and the biggest ONG on the planet.

@JSANTARSIERI

VICXER

ABOUT THIS VOLUME

On this first edition of our ERP security magazine, we will be analyzing one of the aspects that most SAP security newcomers struggle with, *"How can I evaluate if my SAP end users, are actually using a strong password"*

Believe it or not, most organizations have a common problem, they believe that as *Single Sign On* is implemented, the domain should handle password security through global security directives, unfortunately, in many cases, configuring *Single Sign On* in SAP, will do little in terms of preventing an attacker to successfully get plain text passwords.

Join us in our first edition of this ERP security magazine, to know the common pitfalls of SAP password security and how an attacker can crack your SAP hashes even when Single Sign On is activated.

VICXER

VOLUME I

DIFFICULTY: LOW

This volume is recommended for SAP security newcomers and general IT security enthusiasts

BEFORE WE START

VICXER

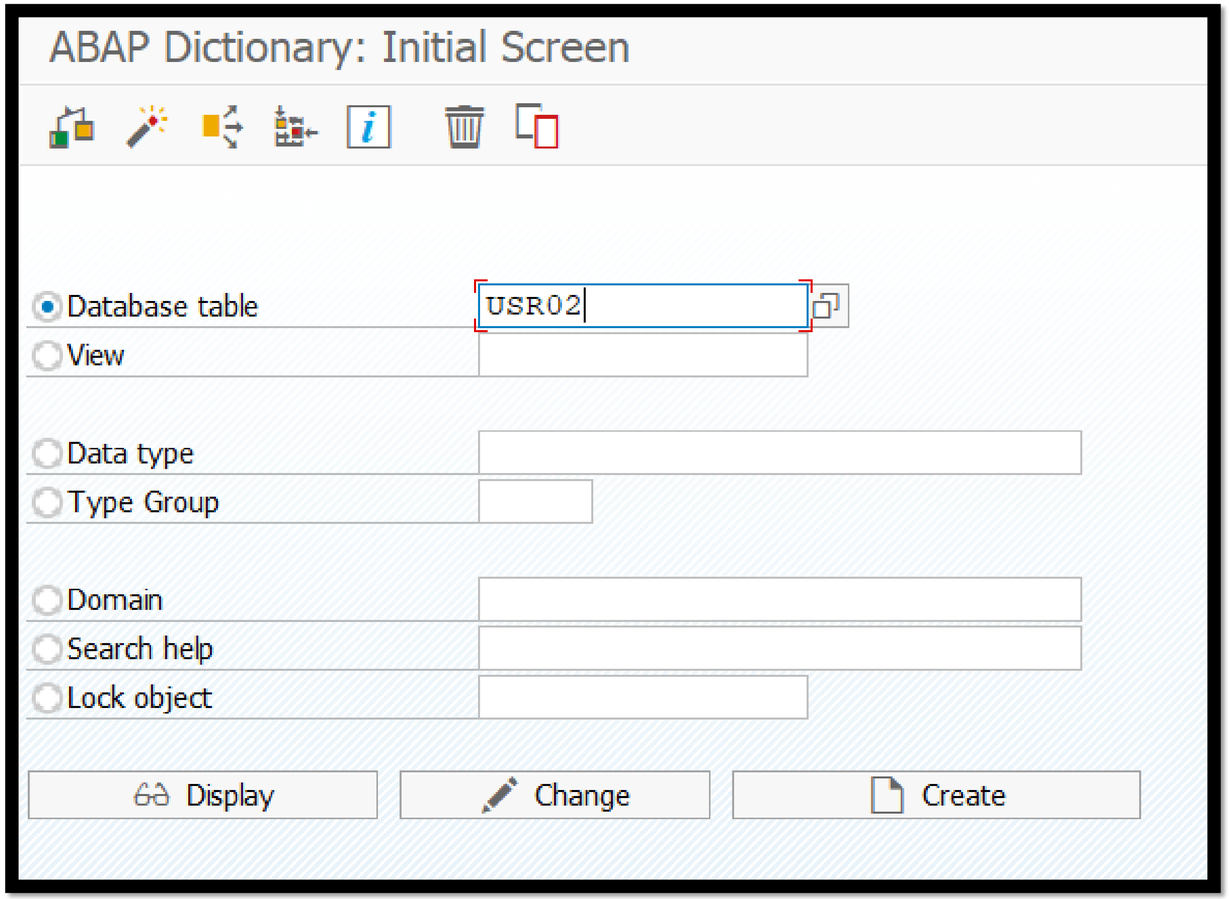
- Make sure you have an SAP GUI installed in your machine, if you do not, you can download a fresh copy from SAP https://wiki.scn.sap.com/wiki/display/ATopics/SAP+GUI+Family, please note that you need to be a valid SAP customer in order to download the SAP GUI from that link. At the time of writing this magazine, the latest SAP GUI version is 7.50

- Finally, you will need **John The Ripper** with *Jumbo Patch*. This special patch is a free add-on to the original **John The Ripper** utility, this add-on contains the different SAP algorithms. You can download this software from the official website http://www.openwall.com/john/

GETTING THE SAP HASHES

VICKER

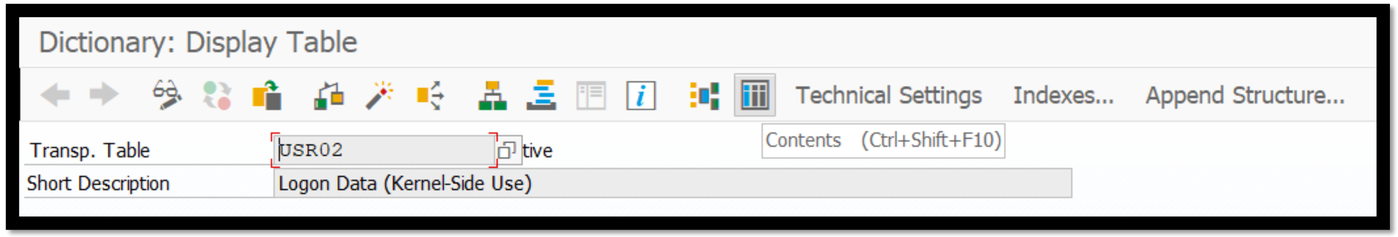
- For this example, we are going to utilize the SAP GUI, login with an administrative account and execute transaction *SE11*, choose table *USR02* and finally, click on *Display*



GETTING THE SAP HASHES

VICXER

- Once inside *SE11*, click on the *Contents* button to actually see the content of the table



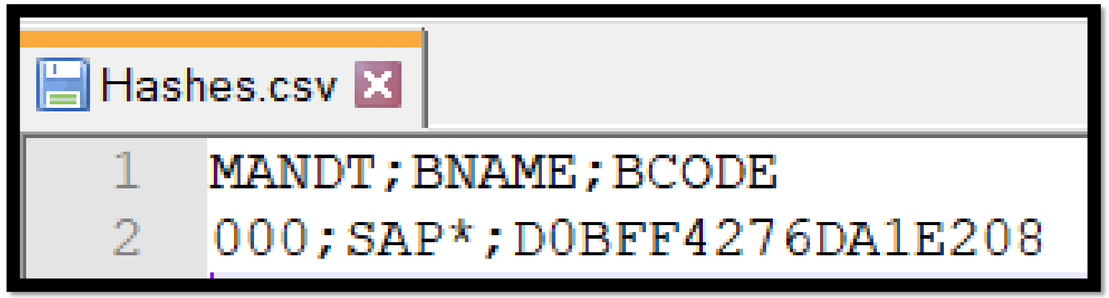
- If SAP asks you what fields you want to display, make sure you select BNAME and BCODE, this last field, will contain the weakest SAP hash, this is exactly what an attacker who had previously compromised the target system will do (a weak algorithm equals a faster cracking process)

- Finally, go to *Edit* and click on *Download*, choose the *Spreadsheet* option (menu options might change depending the SAP GUI version and type)

CRACKING THE SAP HASHES

VICXER

- Our file should look like this (please note that we removed many lines to facilitate comprehension)



- Field MANDT corresponds to the user's client, BNAME is the formal username and BCODE contains the user's hash, all fields are separated with a semi-colon (CSV format)

CRACKING THE SAP HASHES

VICKER

- Now, we need to convert the CSV file to a format that is acceptable by **John The Ripper**, here, we have many options, we can use John's script called ***sap2john.pl*** (comes with the tool) or we can create our own parser script

- John is very particular in terms of format, the correct input is

USERNAME:SALT <40 Empty spaces> $HASH

- After parsing the CSV, your new file should look like this

CRACKING THE SAP HASHES

VICXER

- Once the parsed file is ready (per our example *Clean.txt*) you just need to invoke the cracker by executing the following command ***./john Clean.txt*** (Example is Linux based)
- After a few minutes (depending on the password strength) John The Ripper will present us with a clear text password

```
Warning: SAP-B format should never be UTF-8.
Use --target-encoding=iso-8859-1 or whatever is applicable.
Using default input encoding: UTF-8
Loaded 1 password hash (sapb, SAP CODVN B (BCODE) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
06071992         (SAP*)
```

FINAL CONSIDERATIONS

VICXER

- *“I cannot login with the cracked password”* on this example, we only cracked the SAP ABAP HASH B, depending how SAP is configured (profile parameter *login/password_downwards_compatibility*) SAP might demand the password that comes from a stronger hash

- *“Even if we have weak passwords in SAP, we are protected because we use Single Sign On”*, I hear this statement very often, but in most cases it is absolutely false, even if Single Sign On is enabled, most SAP installations will still allow “direct logons”, it is very important to verify the values of the following profile parameters (*login/disable_password_logon* and *login/password_logon_usergroup*)

QUESTIONS?

VICXER

For more information about this tutorial and our offerings, please visit *https://vicxer.com* or contact us at *info@vicxer.com*

@VICXERSECURITY