CYBERSECURITY

SCANNING AND ENUMERATION: WINDOWS

PREPARATION

Decide on performing live-testing or virtual-testing:

LIVE-TEST

IMPORTANT:

If you perform a live test, it's best to have a backup/image of your system. At least make a backup copy of files you are changing.

In a live test works with the existing users/administrators.

VIRTUAL-TEST

If you will not perform a "live" test:

Download and install Windows 2016 Server or Windows 10 Desktop

Creat users, for example:

Create a disabled admin account.
Create an active admin account.
Create a test-user account.

ALL TESTS

Download and install KALI large.
For a "live" test: put this image on a USB drive to boot from (tool to do this: iso2disk)
For a "virtual" test: link the iso to the CD of the virtual machine you created.

EXERCISE1: HACK PASSWORD

LIVE-TEST

Create a "kali (large)" bootable USB drive.
You can use a tool like "iso2disc" to do this.

VIRTUAL-TEST

Link the "kali (large)" iso-file to your virtual machine's CD-rom drive.
Boot from this live-CD.

Boot into "forensic mode".
Find out how to use the "chntpw" tool to:

a) List all the users from the SAM.
b) Change the password of an existing user.
c) Try to give a non-admin user administrative rights.

Make sure to save the changes & test them afterwards.

EXERCISE 2: COPY SAM

You can perform the same tests on a copied SAM file.

Go to "c:\windows\system32" and copy the SAM & SYSTEM files.
Get these files onto another medium.
Figure out how to do this yourself. One of the options is to start the "ssh service" and connect to do a "secure copy". Many other possibilities exist, depending on live-testing or virtual-testing.

Exercise:
Exchange the SAMs with a collegue. Try to hack the SAM from your standard KALI installation (list users and/or change passwords) and if needed (if you changed a pw) give it back. You can then test if it worked…

Important: Best to make a copy of the original SAM if you go back to the original machine for testing!

EXERCISE 3: CRACK OFFLINE SAM

In exercise 1 & 2 we assume that you get/know the name of a user.
But what if we also wanted to crack the passwords.
How can we tackle this?

Actually this could already be considered part of “exploitation”

OLDER WINDOWS SYSTEMS

Using “chntpw -l” already gives a list of local users.

To get their passwords we will first get the hash.
We use samdump2 to get the users and their hashes.
Samdump needs the SAM and SYSTEM databases from the system.
In my test, some of the usernames didn’t get included with the hash so you need to cross-reference with the chntpw output.

Extra: you could use the “pwdump” tool which does get all the names and hashes.

Check the output from chntpw. Check the output from samdump2.

Note: If you are running a new version of Win10 you can see that all the hashes are the same: “empty”
The security structure has changed after Windows 10 “Anniversary Edition”.
If this is not the case, you can feed the hashes to “john the ripper” as further in this exercise.

NEWER WINDOWS SYSTEMS

We will use “mimikatz” to extract the hashes!

Find & Install “mimikatz” = unzip of the source files.
Warning: this is considered malware by some/all virusscanners.
Possible solutions: allow an exception, switch off real-time scanning (defender) or perform the install (unzip) in a virtual machine. (Be carefull !) → find a way to use “mimikatz”.

Copy the SAM and SYSTEM files into mimikatz/x64.

Run “mimikatz”.
In the command-line check the options for “lsadump”.
mimikatz # lsadump::sam /system:SYSTEMCOPY /sam:SAMCOPY

This gives you the hashes of the users. List them.

UNHASHING THE PASSWORDS

John the ripper = part of KALI.

You found the hashes. Now create the file to input to “john the ripper”, should contain per line:
UserName:Hash

To unhash, run “john --format=NT ./yourhashfile”.

Some extra help:

Cracked passwords can be shown & can later be shown by adding “--show” to the command in the line above. Note: John the ripper works on a hidden directory “.john” an contains all found passwords in “john.pot”.

Note: brute force can take time…

To move faster, create your own wordlist = list of possible passwords… and tell john to use this list through this option: “--wordlist=yourlist”

Document your findings & good luck!
