Badblue exploit and mimikatz dump:

Goal: get hashes from target system, using mimikatz to extract them

Running an nmap service-version scan, a target machine is using a service with badblue 2.72.

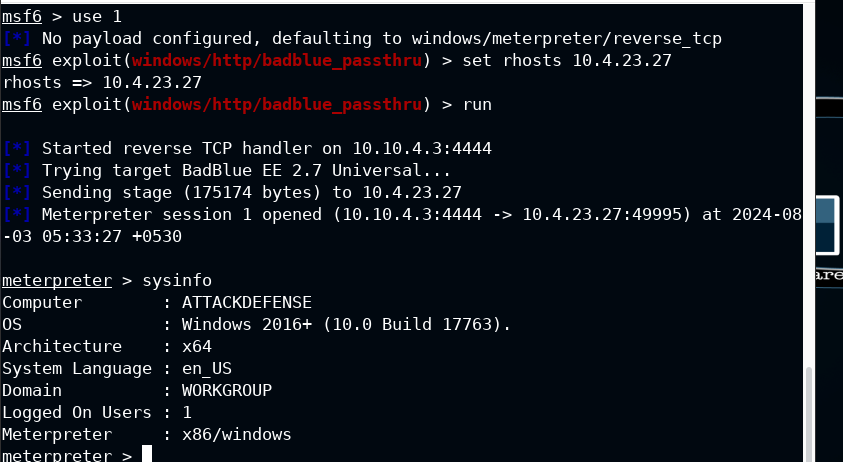
Start by searching Metasploit (msfconsole -q) with the command: search badblue

We ding the appropriate version at option 1.



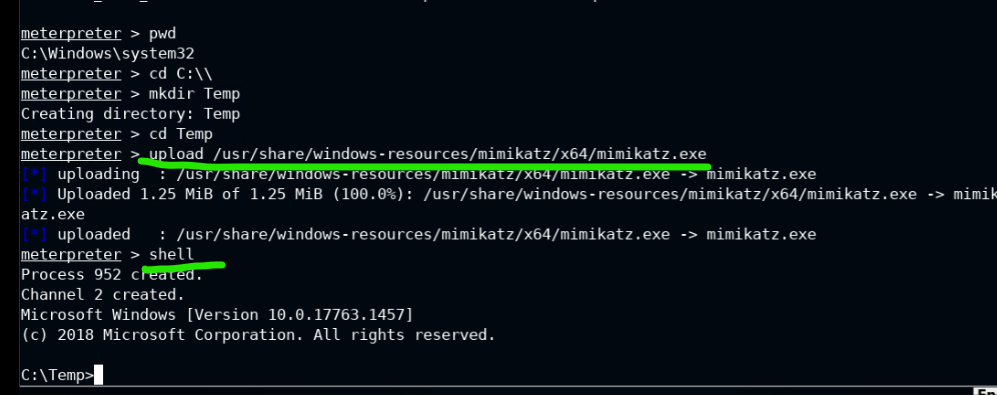
Set the rhosts to the target and run it.

It’s an easy in-road to a meterpreter session, where we can see more sysinfo.



That’s just the warm-up.

We need to upload mimikatz on the target, so let’s go into the main C drive and make the Temp folder. Then we upload out mimikatz into this. Note, this matches the x64 architecture of the target, as seen above in sysinfo.

Then, invoke a shell session 

Invoke the mimikatz.exe program within the shell session.

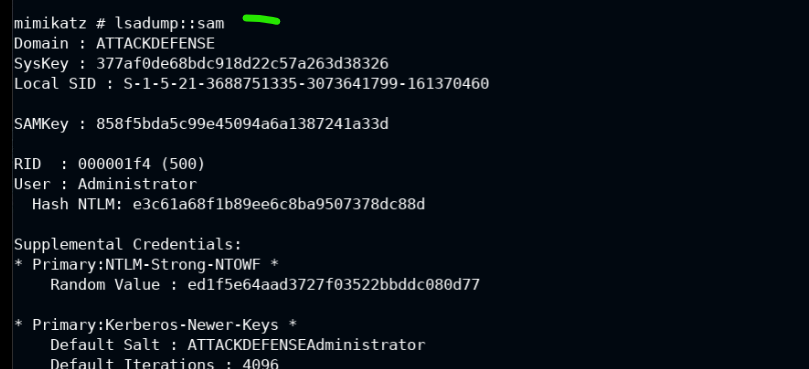


Command : privilege::debug

If it returns with 20 ok, then you can do things freely. We need these privs to run tricky processes.

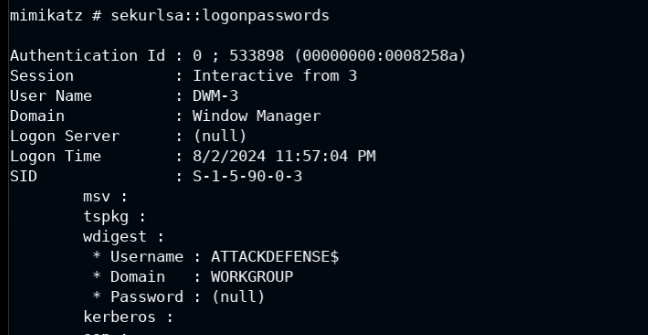
Command: lsadump::sam

This will give us some info. SysKey, SAMKey and NTLM hashes are worth noting

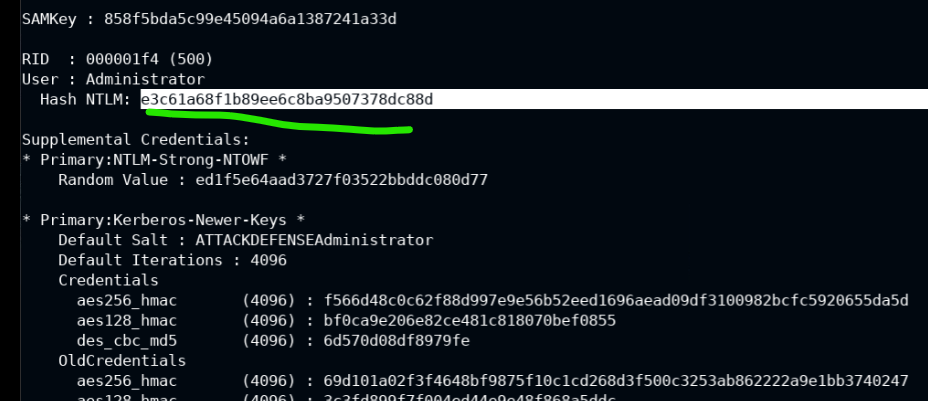


Command: sekurlsa::logonpasswords

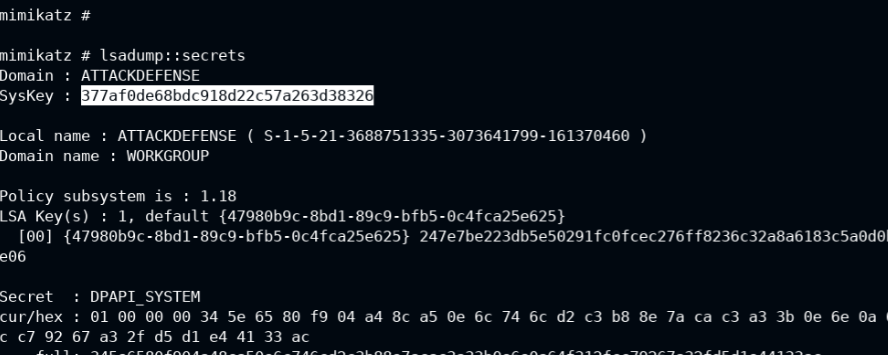
Well, we tried to see if the passwords were in plain text…. They’re not, as sown by null.



Grab any ntlm hashes while we’re here. This is the best loot we can get for now.



Just to make it clear, here’s the syskey that we want to document too



That’s good for now. We can set up a pass-the-hash attack from here.