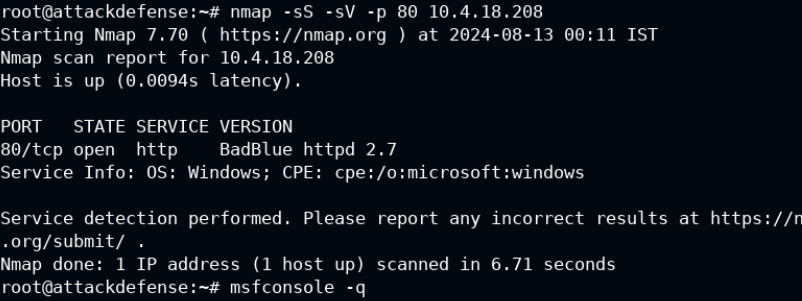
Beginning scenario:we know there’s an http connection running on the target over port 80

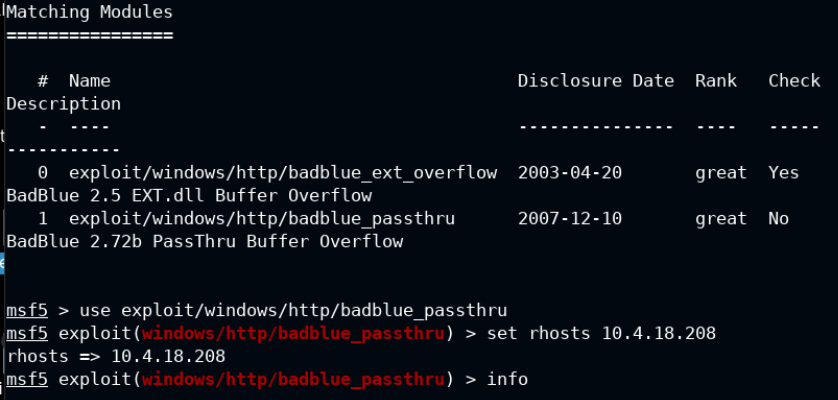
Start with an nmap service versions can of the target’s port 80

We find badblue running, which is associated with an exploit in msfconsole

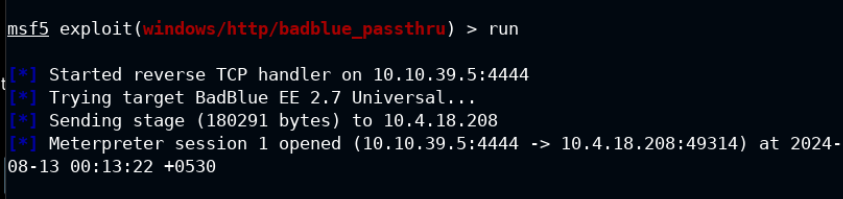


…

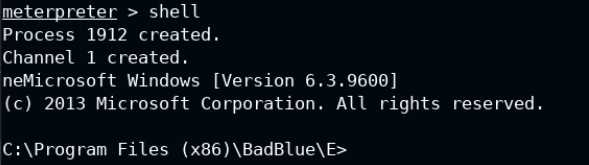
Use the badblue passthru and set rhosts to the target



Run the exploit, which will open a meterpreter session



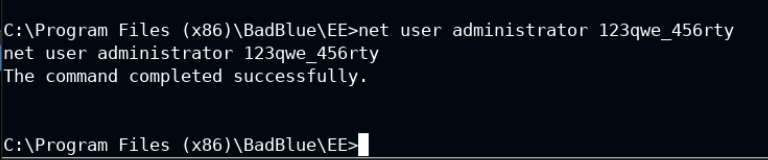
Within meterpreter, open a shell session on the target system



We can change the administrator credentials as follows

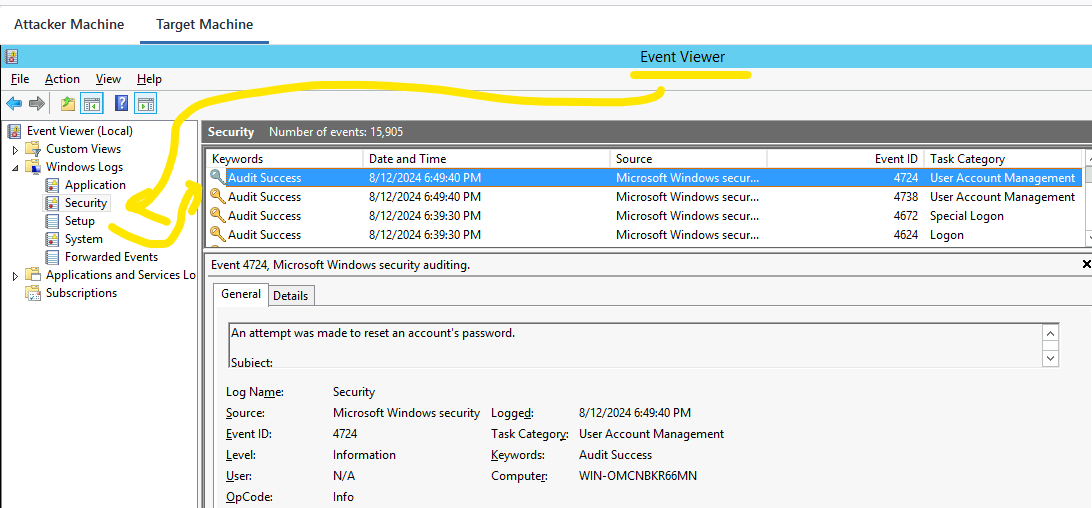
Command: net user existingUsername newPassword

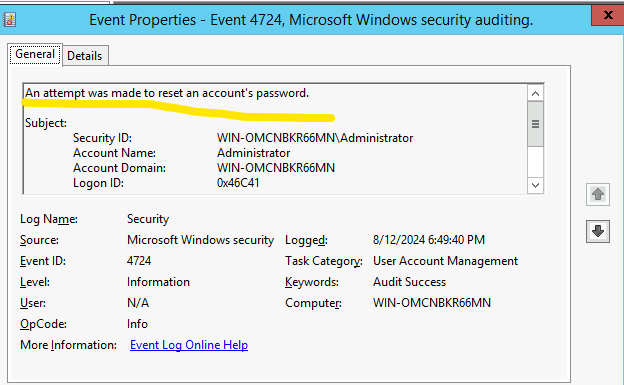
Note: sometimes there will be password policies that force you to include symbols or a certain number of numbers/letters.



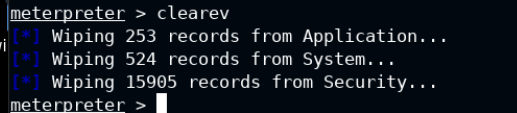
On the target machine, we can see activity in the logs.

This would clue in a defensive team that we made changes, such as altering the admin’s password above



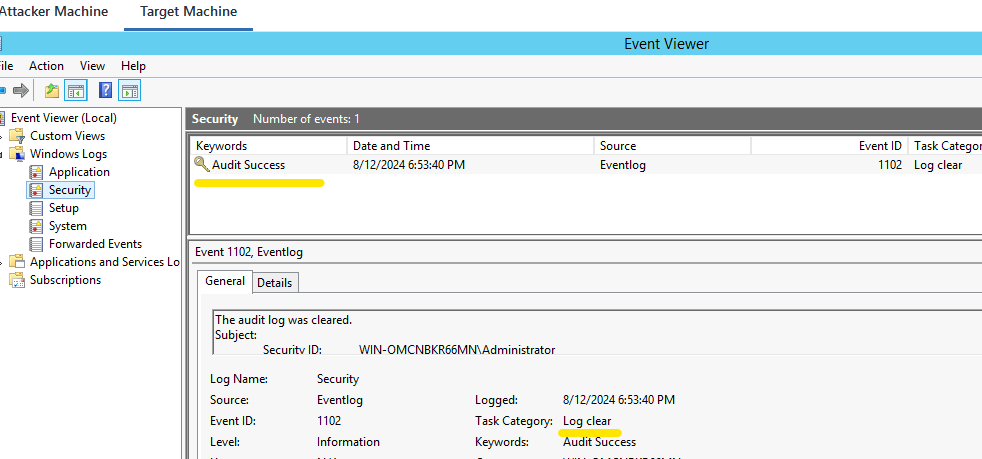
This is what it looks like when you double click an event to open it up. You can see the message underlined, showing our activity, tampering with the password.

The quick meterpreter command to get rid of records is clearev



…

After clearing things, the only log that exists is a note saying the admin did a log clear.



…

Oddly enough, the instructor mentions this as “a bad way to cover your footptints” but fails to discuss any practical methods of actually hiding movement in a practical way. Even after finishing the module, for Metasploit, this issue remains unresolved.   
I cannot, in good faith, recommend INE as an educational organization when all these educational failure keep stacking up one after another.