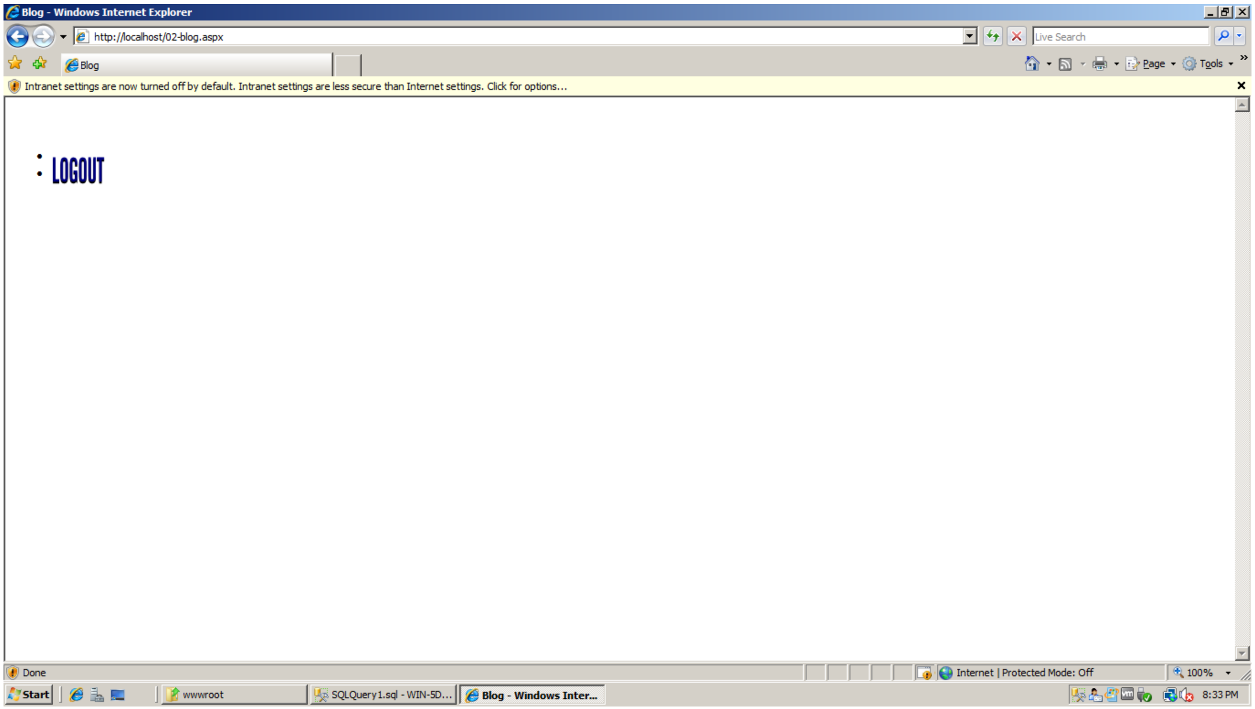
Homework #4: Database Attacks and Defense

- This is an individual assignment, and is worth 30 points.
- The due date is Wednesday, Feb 17th, 4:00 pm.
- You need to provide your answers to the “Homework #4 – Tasks.docx” file. Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Homework #4_ImG.docx). If you do not follow the convention, I will deduct 1.0.
- Do not copy any of the sample screenshots provided as illustrations.
- Each Task is worth six (6) points.
- Use the accompanying **Oldhouse website.zip** and **Oldhouse-Table-Create-HW4.sql**.

- **(Task # 1)** Take a screenshot of the next screen after the attack code. You must see Logout button.

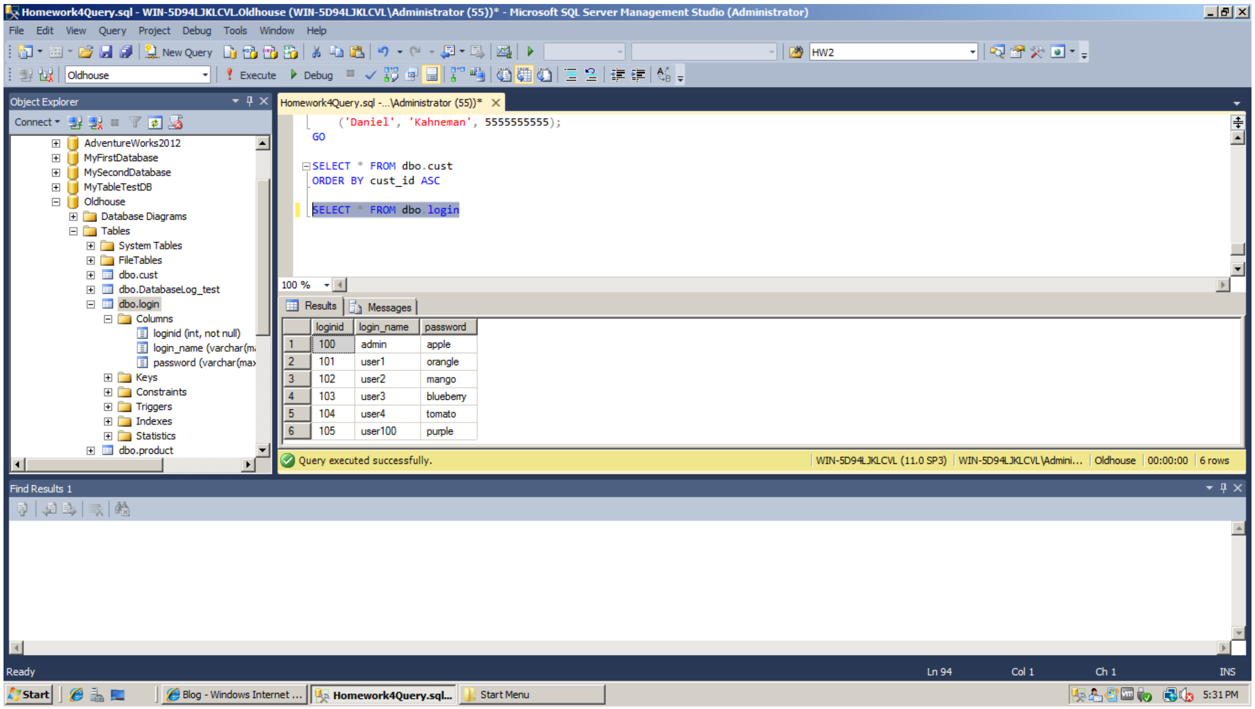

Blog - Windows Internet Explorer
http://localhost/02-blog.aspx
Live Search
Blog
Page
Tools
LOGOUT
Done
Internet | Protected Mode: Off
100%
Start
wwwroot
SQLQuery1.sql - WIN-5D...
Blog - Windows Inter...
8:33 PM

Intranet settings are now turned off by default. Intranet settings are less secure than Internet settings. Click for options...

- **(Task # 2)** Enter the following attack code in **Login name** box and make the Password box blank.

  Task #2A: What is the constructed query that is passed on to SQL Server? If you study the code in **Login.aspx.cs**, you can figure out the constructed query. Also, refer to the class slides for ideas.
  Select * From login
  Where login_name=’admin';
  INSERT INTO login VALUES ('user100','purple') ;--

Task #2B: Go to the SQL Server and run the query below and confirm that the account (‘user100’, ‘purple’) is indeed created in SQL Server. Provide a screenshot.

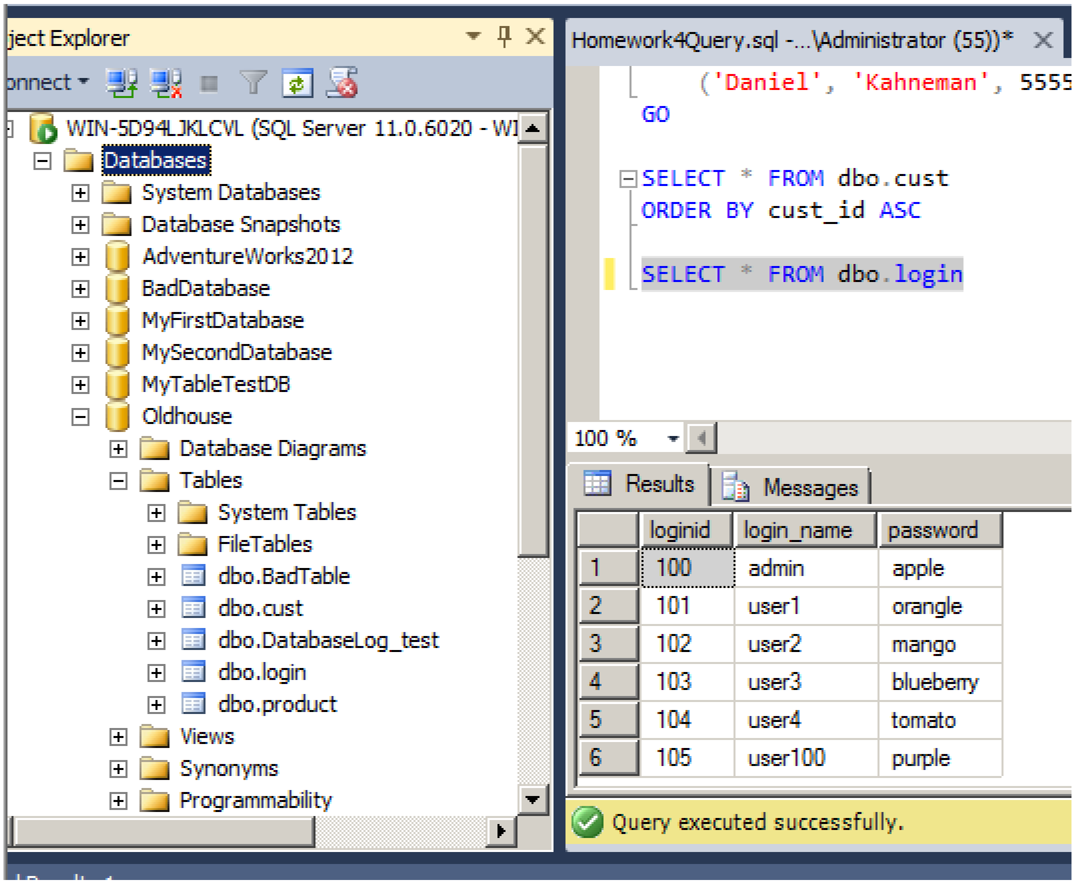


```
    ('Daniel', 'Kahneman', 5555555555);
GO

SELECT * FROM dbo.cust
ORDER BY cust_id ASC

SELECT * FROM dbo.login
```

	loginid	login_name	password
1	100	admin	apple
2	101	user1	orangle
3	102	user2	mango
4	103	user3	blueberry
5	104	user4	tomato
6	105	user100	purple

Query executed successfully. | WIN-5D94LJKLCVL (11.0 SP3) | WIN-5D94LJKLCVL\Admini... | Oldhouse | 00:00:00 | 6 rows

- **(Task # 3)** Enter the following two attack codes using **Login name** box, respectively. Leave the **Password** box empty. Show in screenshots that the database and the table are created. The table will be created in **Oldhouse** database.

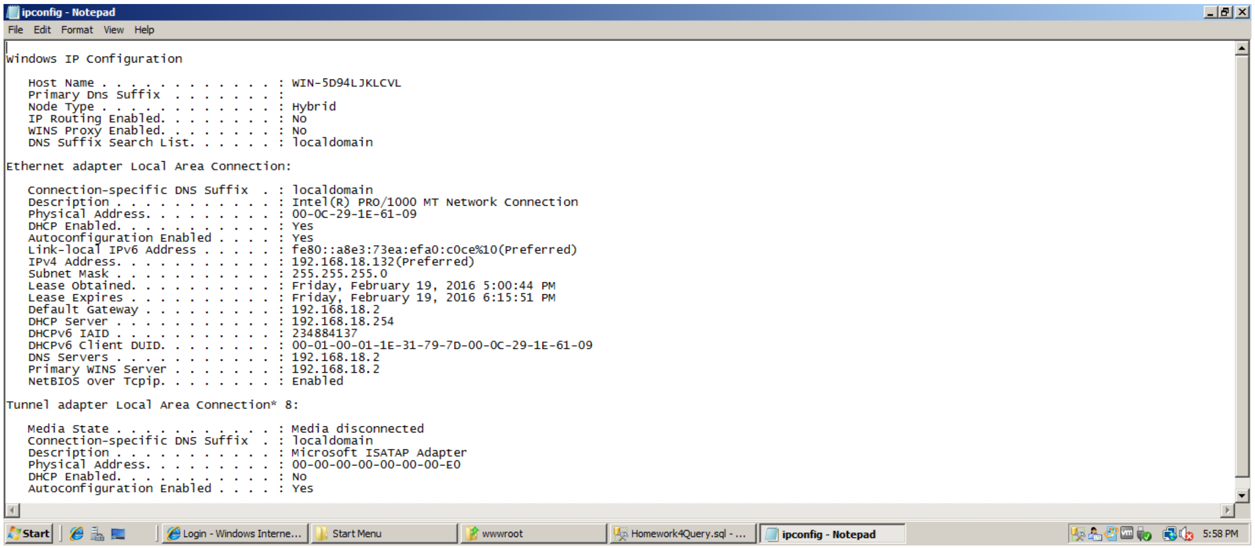


```
    ('Daniel', 'Kahneman', 5555
GO

SELECT * FROM dbo.cust
ORDER BY cust_id ASC

SELECT * FROM dbo.login
```

	loginid	login_name	password
1	100	admin	apple
2	101	user1	orangle
3	102	user2	mango
4	103	user3	blueberry
5	104	user4	tomato
6	105	user100	purple

Query executed successfully.

- **(Task # 4)** Go to the directory **c:\inetpub\wwwroot\** in Windows 2008 Server and locate **ipconfig.txt** file. Open up the file and take a screenshot of its content. After creating a backdoor, you can access the file you have just created (we don't do this part).



```

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-5D94LJKLCVL
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-1E-61-09
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a8e3:73ea:efa0:c0ce%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.18.132(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, February 19, 2016 5:00:44 PM
   Lease Expires . . . . . . . . . . : Friday, February 19, 2016 6:15:51 PM
   Default Gateway . . . . . . . . . : 192.168.18.2
   DHCP Server . . . . . . . . . . . : 192.168.18.254
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-31-79-7D-00-0C-29-1E-61-09
   DNS Servers . . . . . . . . . . . : 192.168.18.2
   Primary WINS Server . . . . . . . : 192.168.18.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

- **(Task # 5)** Take a screenshot of Windows Task manager that is running **ping.exe**. If the ping process disappears quickly, increase the counter 'n'. If you cannot capture the screen, just report it.

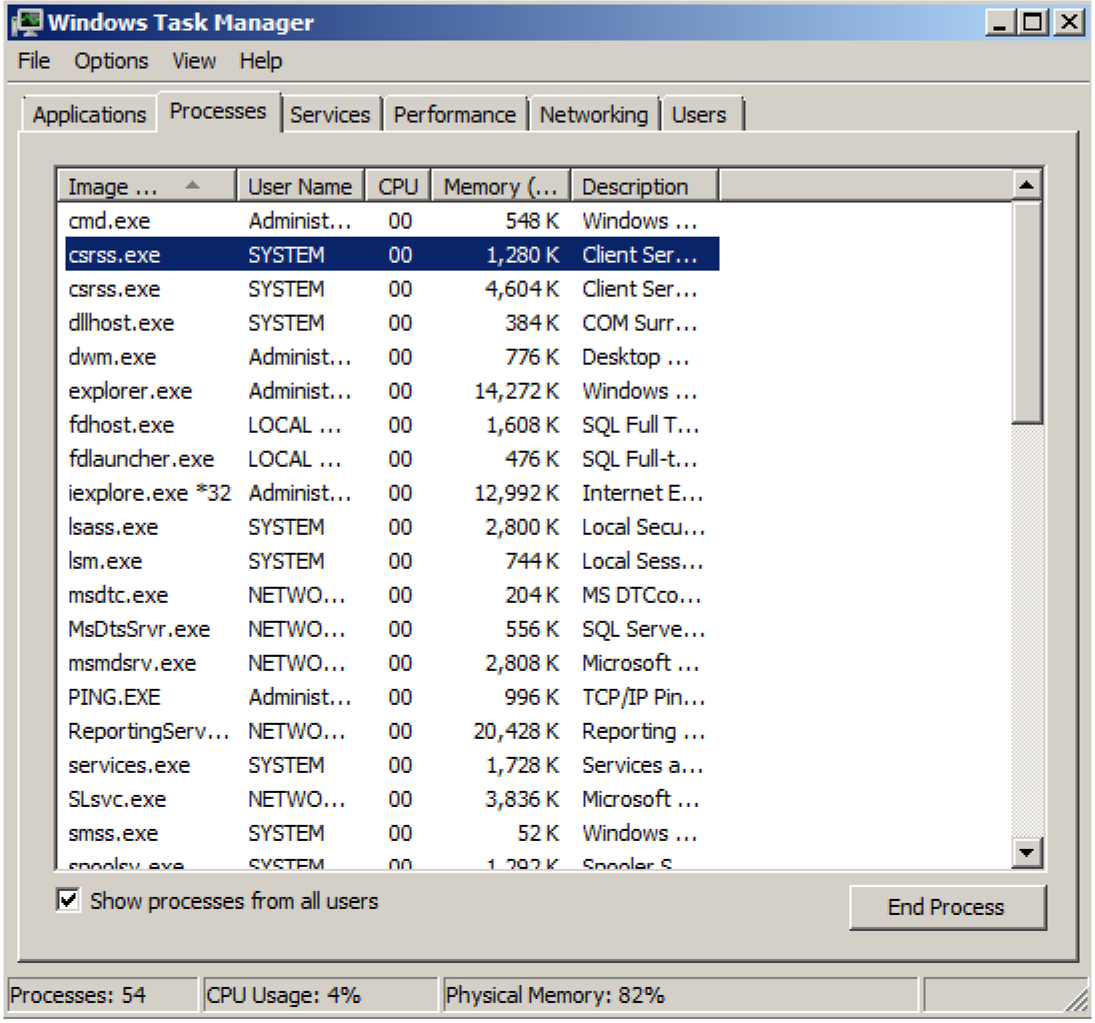


Image ...	User Name	CPU	Memory (...	Description
cmd.exe	Administ...	00	548 K	Windows ...
csrss.exe	SYSTEM	00	1,280 K	Client Ser...
csrss.exe	SYSTEM	00	4,604 K	Client Ser...
dllhost.exe	SYSTEM	00	384 K	COM Surr...
dwm.exe	Administ...	00	776 K	Desktop ...
explorer.exe	Administ...	00	14,272 K	Windows ...
fdhost.exe	LOCAL ...	00	1,608 K	SQL Full T...
fdlauncher.exe	LOCAL ...	00	476 K	SQL Full-t...
iexplore.exe *32	Administ...	00	12,992 K	Internet E...
lsass.exe	SYSTEM	00	2,800 K	Local Secu...
lsm.exe	SYSTEM	00	744 K	Local Sess...
msdtc.exe	NETWO...	00	204 K	MS DTCco...
MsDtsSrvr.exe	NETWO...	00	556 K	SQL Serve...
msmdsrv.exe	NETWO...	00	2,808 K	Microsoft ...
PING.EXE	Administ...	00	996 K	TCP/IP Pin...
ReportingServ...	NETWO...	00	20,428 K	Reporting ...
services.exe	SYSTEM	00	1,728 K	Services a...
SLsvc.exe	NETWO...	00	3,836 K	Microsoft ...
smss.exe	SYSTEM	00	52 K	Windows ...
spoolsv.exe	SYSTEM	00	1,292 K	Spooler S

☑ Show processes from all users

Processes: 54 | CPU Usage: 4% | Physical Memory: 82%