# NTU FYP - WMI Security Progression

1. Research on the technical knowledge needed to manipulate WMI – PoweShell, VBScript, WQL,etc.
2. Learnt Power Shell Manupulation and Scripting on Lynda – Power Shell 5 Essential Training
3. Learnt Basic VB Scripting on YouTube.com – VBScript Basic Series (official)
4. Research on basic WMI manipulation using software like PS, WMIC, wbemtest, WMI Explorer 2.0 and Sapien WMI Explorer
5. Research on WMI class manipulation
6. Research on WMI Consumer, Event Filter and Consumer-Event Binding
7. Understand the technique and code of APT29’s Fileless WMI and PowerShell Backdoors (POSHSPY) Exploitation (Not fully understand yet)
8. Sourcing more article and information on WMI Security

# What is done/can be done now?

1. Using WMI to retrieve sensitive information like process and Service information, OS information, BIOS info, Program installed, Disk info, VM detection, etc. There are more than 8000 WMI classes , so there are a very large amount of data that we can retrieve.
2. Create a WMI based-script to maliciously manipulate all internet browser (Chrome,Firefox,IE and etc.) to open an infected page on lunching broswer. Adding malicious URL at the back of the run path.
3. Inject Payload into WMI classes. Can be encrypted Shell code that listens to C2 Server.
4. Create Event filter, Consumer and Event-Filter Binding. Create a script using VBScript to listen on a C2 Server on Startup Event ( Currently expermenting this )

# Problem Faced / Bottle Neck

1. All the above mentioned technique can only be achieve **IF AND ONLY IF**  I have the privilege credential / access to the system itself.
2. Microsoft do not provide a full documentation on the usage, Architecture and class infomation related to WMI. Most documentation are not complete.