Cyber Security Study Guide

* **If you open a malware file in IDA Pro and determine the purpose of each module, which type of analysis are you performing?**
  + Basic static Analysis
* **If you run strings.exe on a malware file, which type of analysis are you performing?**
  + Basic static Analysis
* **Which type of malware conceals the existence of other code?**
  + Downloader
* **Which item below can be used to conceal the strings in an executable?**
  + **UPX**
* **What type of file is calc.exe?**
  + **ELF**
* **How many bytes are used to store the string HELLO in Unicode?**
  + **5 Bytes**
* **Which library is the interface to the Windows kernel?**
  + **Kernel32.dll**
* **Which PE section contains CPU instructions?**
  + **.rsrc**
* **Which tool reveals which services are hosted by each instance of scvhost?**
  + **Procmon**
* **Which tool is specifically intended to aid analysis of the network traffic from malware?**
  + **INetSim**
* **Which type of language contains commands like this?  
  xor eax,eax**
  + **Low-level language**
* **Which memory section contains objects created by the malloc() function?**
  + **Heap**
* **Which register points to the top of the stack?**
  + **%ebp**
* **What is the value in eax after these instructions?  
  mov ebx, 0x10  
  mov eax, ebx  
  inc ebx**
  + **0x11**