**ASLR and Antivirus**

**Address Space Layout Randomisation**

This randomises the offset of core apps so they are not located in the same spot in memory every time

* This includes the stack, heap and shared library
* Done on start-up/reboot

Done to prevent exploits

**Why is it important?**

When building exploits or even running a prebuilt one, understand that this may be in place

* If an exploit works once and then after a reboot it stops working, this may be the issue

**Can it be bypassed?**

Yes

* ROP Chains
* Partial EIP Overwrite
* **Abusing non-ASLR libraries**
* **Single Bit Overwrite**

**Anti-Virus**

**A tool designed to identify malicious intent from the user or applications**

* Normally resides at the kernel level
  + Or SYSTEM space in Windows

Most enterprises have AV installed in some way shape or form

* When attacking a machine**, knowing if there is one and what kind it is will help you greatly when trying to be undetected**
* Dumping over netcat, a meterpreter shell or anything like that, an AV will flag it immediately
  + Delete the process, quarantine it and/or notify the admin

Even randomly firing off exploits or running an attacker’s binary on a comprised system may tip off admins

**An AV can run a number of different checks**

* Sandbox the application
* Signature based
* Heuristics based
  + Runs in a really restricted sandbox to see what type of calls the app is trying to do
  + Identifies malicious behavior

**BUT, they *can* be bypassed**