**Young Jun Kim**

**Block C**

**April 3, 2017**

**What is an 0day (zero day) exploit?**

vulnerability in your computer to exploit anything in your computer as long as it is turned on and no way to protect against it.

**How many 0 days did Stuxnet have?**

four 0days

**What is SCADA?**

Technology that is controlling robots, and power plants, etc.

**What is a PLC?**

programmable logic controllers

**What was Stuxnet designed to do?**

Stuxnet targets PLCs which allowed the automation of mechanical processes such as those used to control machines in factory assembly lines, amusement rides, or for separating nuclear material.

**How exactly did Stuxnet work?**

Infection > Search > Update > Compromise > Control > Deceive and Destroy

**How did Stuxnet hide itself?**

It hid by faking as a windows operating system. No One noticed.

**How was Stuxnet unstoppable?**

Once the virus was spread there was no way to stop it.

**What does it mean when a network is ‘air-gapped’?**

It meant that unsecured networks could take control of another network.

**How did Stuxnet jump the ‘air-gap’?**

Stuxnet jumped the air gaps by travelling in a usb stick that was placed into the computer of someone.

**What happened to the Natanz nuclear facility?**

The Natanz facility shut down shortly after a group of programmers exposed stuxnet.

**Is the Stuxnet malicious code still a threat?**

It is a threat to civilians with no programming background but it has been exposed from professionals.