Malware Review

What is a virus? What happens when its executed? How does it work? What are the phases of a virus?

* 12, 13, 14

What is a virus structure? What are the types of viruses? What is a macro and how does it spread?

* 15, 16, 17

What are some antivirus approaches? What are the 4 generations of antivirus software?

* 19

What is a worm and how does it usually spread? What was the internet worm, how did it work and how did it spread?

* 21, 22, 23

Describe the Code Red 1 and 2 viruses and difference between them.

* 26, 27, 30

How do you design a fast spreading worm?

* 29

What was Nimda? How did it spread and why was it so hard to beat?

* 32, 33

What was the slammer/sapphire worm? Why was it so devastating? What kind of worm was slammer and what was the secret to its speed?

* 34, 35, 37, 38, 39

What is a centralized botnet? What is the life-cycle of an IRC-Based Botnet? What is a distributed Botnet?

* 59, 61, 64

What are the differences in Design complexity, channel type, message latency, detectability and resilience between centralized and distributed botnets?

* 70

What is a Sybil attack?

* Paper exam review