============Start lecture 4 notes==========================

Q.What is the major difference between worms and viruses?

A worm is self-replicating malware that travels through a network without the assistance of a host application or user interaction. • A worm resides in memory and can use different transport protocols to travel over a network

Virus: A virus is malicious code that attaches itself to an application and runs when the application is started.

The difference between viruses and worms is that by definition a virus infects executable host file, programs or operating system and a worm replicates or spreads across a network on its own. These days a large majority of malware is both a virus and a worm. • Both of them have malicious payload to carry out its targeted goal.

Q. What is an ODE (0 Day Exploit) worm?

• We might not be so lucky in the future. We'll see worms with zero-day exploits which means that they are brand new and have been available for zero days.

• Unfortunately, no patches will be available and researchers will need time to understand how these worms work.

• Widespread prevention will become very difficult or in some cases impossible.

Q. Distinguish between a polymorphic and a metamorphic worm. Which are more difficult to deal with?

Polymorphic Worms

• Polymorphic programs dynamically change their appearance each time they run, by scrambling their code.

• The attackers use different code instructions that perform the same function.

• The code morphs into different mutations so that it no longer matches detection signatures.

• The worm will have a different appearance on each victim, making it more difficult to detect and analyse.

Metamorphic Worms

• In addition to changing their appearance, new worms will also change their behaviour dynamically.

• Worms will contain encrypted/obfuscated payloads.

• After a given event occurs (time duration, infection rate or some other trigger), the worm will morph by decoding the hidden functionality. It will hide it's real purpose. (Backdoor, information stealing, DDoS).

• If we catch the original worm we won't be able to determine its true purpose and this makes reverse engineering very difficult.

Q. What is a multi-exploit worm?

Multi-Exploit Worms

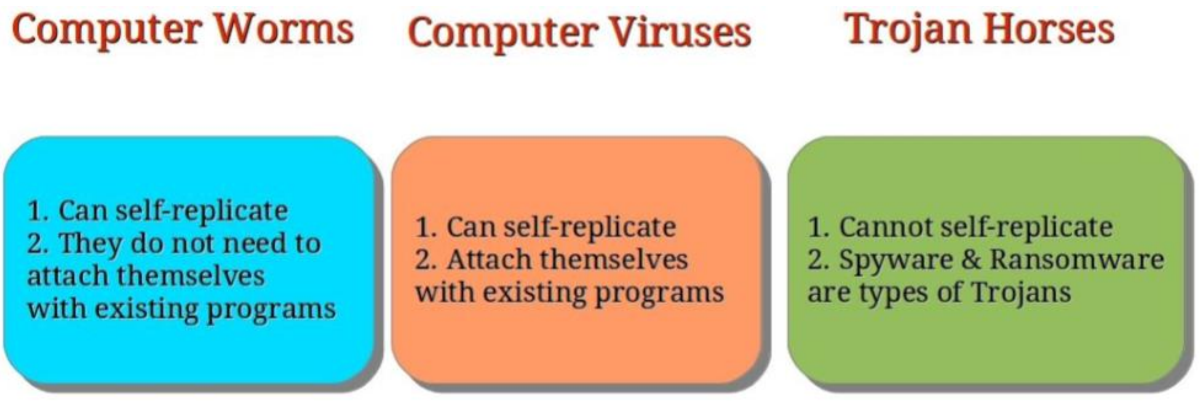
- A worm will use its exploit warhead to exploit a computer.
- Starting out, most worms had only one or two exploits built in – Witty, Sasser, etc
- Nimda had 12 (buffer overflows, browser vulnerabilities, email problems etc)
- New Worms will look to replicate the Nimda model with dozens of ways to penetrate systems.
- If you have patched against N-1 vulnerabilities, the worm will still get in to your system through hole N.

Q. Give an account of Flash Technique in relation to worm.

➢ An attacker pre-scans the Internet for machines which would be vulnerable to the exploit code that will later be loaded into the worm. • The attacker will locate thousands or tens of thousands of vulnerable systems. • Then using a list of the addresses of these machines, the attacker will pre-program the worm with its first set of victims. • The worm is then unleashed on those known victims with high bandwidth closest to the Internet backbone. • It will immediately populate the systems already pre-scanned for the vulnerability.

Q. List steps you can take to safeguard against worm attacks?

• Buffer overflow defences help a lot here. Non-executable system stack prevents 80% of buffer overflow attacks – Windows, Solaris and Linux • Having a process for rapidly testing and deploying patches when they become available. • Anti-virus solutions updated daily • Linking your incident response capabilities with network management in case you need to cut off segments of your network in real time. • Encrypt data on your hard drives. At least then if it is stolen it can not be read by the attacker.



Computer Worms

1. Can self-replicate
2. They do not need to attach themselves with existing programs

Computer Viruses

1. Can self-replicate
2. Attach themselves with existing programs

Trojan Horses

1. Cannot self-replicate
2. Spyware & Ransomware are types of Trojans