Environment preparation

1. Download VM from course study materials, unpack to your computer and import to VirtualBox/VMWare
2. Analysis tools are already installed – Wireshark, procmon, Process Explorer, Autoruns
3. Malware samples are placed in a folder on Desktop

Execute analysis

1. Save snapshot before starting the analysis!
2. Run a tool
3. Stop recording
4. Clear the log
5. Start recording
6. Execute malware
7. Wait 15-30 seconds
8. Stop recording
9. Review log, make notes
10. Restore snapshot

Malware types

- Trojan – Malware masquerading as a legitimate application.
- FakeAV – Malware masquerading as a fake antivirus. The user is persuaded that his computer was infected and the infection can be removed only with premium (i.e., paid) version of fake AV.
- Dropper – Program that contains one or more malware samples and that installs them on a target computer.
- Downloader – Program that downloads and installs further malware on the target system.
- InfoStealer – Malware designed to extract sensitive information and deliver it to an attacker controlled system.
- Ransomware – Malware that threatens the user (e.g., with fake legal notice or with fear that the user could lose his data) and promises to remove the threat when paid a compensatory fee.
- Rootkit – Malware that tries to stay hidden inside the system by hijacking system calls.
- Spambot – Malware designed to send spam.
- DoSbot – Malware designed to perform denial of service attacks.
- Keylogger – Malware that monitors pressed keys, usually with the purpose to reveal user's passwords. In broader sense it is malware that can also take screenshots, copy clipboard content and monitor computer surroundings via webcam or microphone.
- Backdoor – Malware component that allows the attacker to maintain access to the infected computer.
- Worm – Malware replicating itself through network.
- Virus – Malware that attaches itself to legitimate files.

Malware delivery

- USB – Infecting a computer after an external device was attached either when autorun is allowed or after the user opens infected file.
- Email attachement – Opening infected email attachement.
- Drive-by download – Exploiting user computer when he is visiting a compromised website.
- Phishing – Masquerading as a trustworthy entity and persuading user to open some file.
- Warez – Malware is encapsulated within warez files or archives.
- Worm – Worm is replicating through network on its own.

Kill chain

1. Reconnaissance – Searching for targets. Can range from automated scanning in case of worms to getting personal data about important company people in case of spearphishing.
2. Exploitation – Applying exploit code to a target computer in order to exploit existing weaknesses and gain a rudimentary access (i.e., An ability to execute own code, usually malware installer.)
3. Installation – Placement of malware's files on the target computer. Usually temporary files are created and subsequently deleted. System files may be altered or replaced with malware versions.
4. Persistence – Process of assuring that the malware will be executed again. Link to malware can be placed to special registry keys, Startup/Logon folder or into Scheduled tasks.
5. C2 – Network message to a malware-controlling entity. Malware can inform about successful infection, accept new commands, update itself with new version or exfiltrate collected data.
6. Deletion – Removal of all malware traces once the purpose of infection has been fulfilled. May include deletion of system logs or even of all data in the computer. The aim is to make post-incident analysis as difficult as possible.