The Security Threat Landscape

- **Threat:** has the potential to cause harm to an IT asset.
- **Vulnerability:** a weakness that compromises the security or functionality of a system.
- **Exploit:** uses a weakness to compromise the security or functionality of a system.
- **Risk:** the likelihood of a successful attack.
- **Mitigation:** techniques to eliminate or reduce the potential of and seriousness of an attack.

Malware

- Malware is malicious software, including:
- **Viruses:** software which inserts itself into other software and can spread from computer to computer. Requires human action to spread.
- **Worms:** a self-propagating virus that can replicate itself.
- **Trojan horses:** malicious software which looks legitimate to trick humans into triggering it. Often installs back doors.
- **Ransomware:** Encrypts data with the attacker’s key and asks the victim to pay a ransom to obtain the key.

Hacking Tools

- Many hacking toolsets are available
- Penetration testers use the same tools as hackers to test for vulnerabilities
- Hacking tools typically run on Linux

Tools include:

- Password cracking tools
- Sniffers
- Ping sweepers
- Port and vulnerability scanners

Script Kiddies and Targeted Attacks

- ‘Script Kiddies’ is a derogatory term for low skilled attackers who download and use off-the-shelf hacking software to launch exploits.
- They will typically attempt to exploit any vulnerable host they can connect to.
- The attacks are mostly not targeted against a particular individual or organisation.
- More skilled attackers will also look for random victims in order to meet their goals, such as installing ransomware or a botnet.
- Organisations are constantly under these type of attacks.

Targeted Attacks

- Targeted attacks are directed against a particular individual or organisation.
- This type of attack is rarer.
- Skilled attackers will typically start off with very stealthy and low impact reconnaissance, and systematically escalate the attack from there.

Evolution of a Targeted Attack

- External reconnaissance
- Initial compromise
- Escalation of privileges
- Internal reconnaissance
- Further compromise
- Further escalation of privileges
- End goal