

- Filename: eccouncil-ceh31250-v12-1-4-1-information-warfare.md
- Show Name: CEHv12 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Information Warfare

Information Warfare

Objectives:

- Define "Information Warfare"
- List and define IW strategies

-
- What is Information Warfare?
 - Attempting to gain a competitive advantage through attacks against target's IT systems
 - The term 'Information Warfare' is a bit generic and it breaks down into types or categories?
 - C2 Warfare
 - The control over compromised target systems with centralized management
 - The effect or influence they can have on the target
 - Intelligence-based
 - [t]he design and protection of systems that seek sufficient knowledge to dominate the battlespace, and the denial of such knowledge to the adversary.
 - https://itlaw.wikia.org/wiki/Intelligence-based_warfare
 - Electronic
 - Interrupting/degrading/stopping the means of electronic communication
 - aka 'Jamming'
 - Psychological
 - Attacking the morale and mental resolve of opponent
 - Attempt to get the opponent to GIVE UP
 - Propaganda
 - Terrorism
 - Hacker
 - 'Soldiers' of Information Warfare
 - Attack target systems (DoS/DDoS)
 - Theft of data and/or systems
 - Disinformation campaigns
 - Economic
 - Interfere with target's economic/financial capabilities
 - Weaken target's economy
 - Theft of IP
 - Reputational Influence
 - Cyberwarfare
 - Similar to Information Warfare in it's definition
 - Includes
 - Information Terrorism
 - Semantic attacks

- Take over of target system by where the appearance of normal operation is maintained
 - Simulated warfare (wargames)
 - 'Sabre Rattling'
 - Open display of weapons acquisition/capabilities
- What Information Warfare strategies do we need to be aware of?
 - Defensive IW
 - Detection/Prevention
 - Alerts
 - Response
 - Deterrents
 - Emergency Preparedness
 - Offensive IW
 - Web Attacks
 - System hacking
 - MiTM/Replay/Session Hijacking