DECEPTION WORKSHOP NOTES

Attack tools / techniques

- Responder for LLMNR / mDNS poisoning.
- Mimikatz for dumping credentials and secrets out of Windows.
- Lazagne for dumping application specific credentials.
- PowerSploit Swiss Army knife for PowerShell based privilege escalation / lateral movement and data-theft attacks.
- SPN scanning to find interesting hosts in Active Directory.
- Kerberoasting to crack service accounts in Active Directory.
- GPP password cracking to find and crack locally set group policy passwords.

Deception tools

Network services

- Cowrie - Cowrie is an SSH honeypot based off an earlier favourite called Kippo. It will emulate an interactive SSH server with customisable responses to commands.
- Dionaea is a multi-protocol honeypot that covers everything from FTP to SIP (VoIP attacks). Where it really excels is for SMB decoys. It can even simulate malware payload execution using LibEmu to analyse multi-part stagers.

IOT (Internet of Things) decoys

- Honeything emulates the TR-069 WAN management protocol, as well as a RomPager web-server, with vulnerabilities. Other IoT decoys can be created by emulating embedded telnet / FTP servers.

SCADA/ICS decoys

- ConPot emulates a number of operational technology control systems infrastructure, including protocols like MODBUS, DNP3 and BACNET. It comes with a web-server that can emulate a SCADA HMI as well.

- GasPot emulates a Veeder Root Gaurdian AST that is commonly used for monitoring in the oil and gas industry.

Database and NoSQL honeypots

- MongoDB-HoneyProxy emulates an insecure MongoDB database.

- ElasticHoney emulates an ElasticSearch instance, and looks for attempted remote code execution.

Credential honeypots and honeytokens

- DCEPT by Dell SecureWorks places deceptive credentials in Microsoft's Active Directory.

- SpoofSpotter - LLMNR / mDNS poisoning detection on the local subnet.

All-in-One

- Honeydrive is a GNU/Linux distribution that comes pre-installed with a lot of active defence capabilities. Consider it the anti-Kali.

- MHN combines Snort, Kippo, Dionaea and Conpot, and wraps them for easy installation and use.

- Cuckoo Sandbox is not a honeypot, but a sandbox to analyse malware automatically. Malware samples from other honeypots can be automatically submitted to Cuckoo for analysis.

Strategy

- 7 Deadly Sins - How to Fail at Implementing Deception

- Adversarial thinking