Příloha 4.4 – Technická specifikace k části 4 VZ

Část 4 veřejné zakázky – IT bezpečnost

Network Security – Hacking v praxi II

Délka kurzu: 5 dnů

Počet účastníků: 1

Náplň kurzu:

Systémové útoky

- Zneužívání nejčastějších chyb v administraci ke kompletní kompromitaci sítě
- Proč může nevinné přesměrování lokálních zdrojů v RDP vést k ovládnutí sítě
- RDP MitM a session recording aneb vzdálený záznam klávesnice a obrazovky admina
- Chybné používání identit pro administraci, spuštění úloh a služeb
- Offline útoky pro ovládnutí domény
- Hesla a vykrádání tajemství z počítačů
- Zneužívání shadowcopy pro vykrádání databází, Active Directory a file serverů
- Zneužívání lokálních účtů ve výchozím nastavení
- Vykrádání paměti počítače
- Vykrádání profilů a šifrovacích tajemství
- Pass The Hash aneb jak s údaji z paměti ovládnout vzdálené systémy a proč není třeba lámat hesla
- NTLM Relay aneb jak položit zcela vzdálené systémy, kam nikdo nechtěl přistupovat jen během útoků MitM
- Responder a podvrh legitimních cílů aneb jak snadno nalákat oběť a zneužít její výchozí nastavení
- Pass The Ticket aneb vykrádání Kerberosu
- Kerb roasting aneb kompromitace účtů služeb
- Golden Ticket prakticky - průstřel celého AD forestu pomocí jediné domény
- DMA útoky aneb jak obejít ochranu BitLocker

Malware, jak ovládnout firmu na dálku, útoky zevnitř Princip komunikace a proč útoky zevnitř vedou

- Jak zneužít nejčastější cesty spuštění malwaru k infiltraci prostředí
- Možnosti ovládání a sledování obětí
- Skrývání malware - kam se skrýt, aby vás nikdo nehledal
    - Wmi filtry
    - Využívání více úrovní streamů
- Opomíjená nastavení office
- Skrývání v registrech
- Šifrování
- Neobvyklé metody spouštění kódu
- Využívání skrytých kanálů a tuneling v jiných protokolech
- Pivoting aneb jak prostoupit z napadeného počítače dál do nepřístupného prostředí
- Automatizace prostupu prostředím
- Infekce obsahu při MitM útocích
- Fileless backdooring
- Asynchronní komunikace
- Skrývání malwaru pomocí Application Compatibility Toolkitu a tvorba shimů

USB Hid útoky aneb jak zneužít cokoli v USB ke kompletní kompromitaci systému

- Falešné USB flash disky dynamicky měnící svůj obsah pro ovládnutí sítě
- Způsob vytváření objektů na HID sběrnici
- Ovládání počítačů pomocí HID injection
- Způsoby zcizení síťového provozu a SSL inspekce
- Přihlášení k systému bez fyzického přístupu
- Reverzní SSH tunel pro ovládnutí počítače
- Kali Nethunter jako penetrační platforma
- P4wnP1 a BashBunny jako prostředek pro penetrační testování

MouseJacking a KeyJacking

- Zneužívání zranitelných klávesnic a myší pro ovládnutí vzdálených počítačů

Úvod do Android Hackingu

- Generování malwaru pro mobilní prostředí
- Prostřelování slabin na zastaralých systémech
- Zneužívání oprávnění aplikací
- Možnosti sledování mobilních zařízení
-

DoS attacks

- Flooding cílů
- Reflection attacks
- Amplification effect