Tárgytematika / Course Description
Etikus hackelés alapjai

SAPL_AUTM621

Tárgyfelelős neve / Teacher's name: dr. Hidvégi Timót
Félév / Semester: 2024/25/1
Beszámolási forma / Assesment: Teljesítve
Tárgy heti óraszáma / Teaching hours(week): 0/0/0
Tárgy féléves óraszáma / Teaching hours(sem.): 24/0/0

OKTATÁS CÉLJA / AIM OF THE COURSE

Biztonságtudatosság fontosságának hangsúlyozása, alkalmazása

Biztonságtudatosság, szemléletmód kialakítása a résztvevőknél (pl.: ne használjanak egyszerű jelszavakat, alkalmazzák a 2FA-t, stb)

A különböző alapfogalmak definícióinak a megismertetése (pl.: hackerek típusai, célok, sérülékenységek keresése, sérülékenységkeresés vs pentest, stb.), a törvényi háttér részletes bemutatása

IT protokollok megismerése, tulajdonságainak (esetleg a hibáinak) a "kihasználása"

Számítógéphálózatok alapjainak a megismerése sérülékenységkeresés (és kihasználásának) szempontjából

Speciális szoftverek használatának a megismerése, alkalmazásának alapjai

TANTÁRGY TARTALMA / DESCRIPTION

1. alkalom	Bevezetés, a tanfolyam szerepének és fontosságának a bemutatása 1. fogalmak tisztázása, törvényi háttér 2. Támadások típusai, támadási vektorok 3. Speciális Linux disztribúciók bemutatása 3.1 Kali Linux alapjai 4. Tesztkörnyezet szerepe, miért fontos a használata 4.1 Tesztkörnyezet létrehozása, a virtuális gépek szerepe a tanulásban 4.2 Áldozatgép szerepének az ismertetése, lehetőségek 4.3 Saját hálózat létrehozása, a pivoting lehetőségének megteremtése
2. alkalom	Főbb IT protokollok bemutatása, néhány tulajdonságuk megismerése és azok kiaknázása. A résztvevők megismerik még az egyik legnépszerűbb hálózati monitoralkalmazást, a Wireshark használatának alapjait. 1. Hálózatok felépítése 2. OSI modell 3. TCP, UDP, ICMP, ARP protokollok bemutatása, alkalmazása 4. Különböző kisebb alkalmazások készítése Scapy nélkül és Scapy-vel (Python nyelv kerül alkalmazásra) 5. A hálózati forgalom figyelése Wireshark programmal, a Wireshark megismerése

3. alkalom	Egy sikeres támadáshoz (vizsgálathoz) elengedhetetlen a célpont minél részletesebb megismerése. Ebben segít a nyílt hozzáférésű adatbázisokban lévő keresés, amelyet OSINT-nak neveznek. OSINT alapok, sock puppet (avatar készítése, azaz, elrejtőzés az Interneten) készítése, információk begyűjtése személyről, szervezetről, szolgáltatásról
4. alkalom	További felderítési technikák, információgyűjtési eljárások kerülnek ebben a blokkban bemutatásra. 1. Keresők alkalmazása, Google, shodan, wigle, stb 2. Portscannerek (pl.: nmap) bemutatása, alkalmazása 3. Sérülékenységek, verziószámok keresése 4. Sérülékenységek osztályozása, Nessus telepítése, alkalmazása 5. Hálózatbiztonságban lévő néhány sérülékenység 6. Egy egyszerű portscanner készítése Python/C# nyelven
5. alkalom	MITRE ATT@CK keretrendszer Metasploit bevezető, alkalmazása, Főbb Meterpreter parancsok Sérülékenységek hatása, kihasználása Exploitok alkalmazása néhány szolgáltatásra
6. alkalom	Ebben a blokkban áttekintjük a jelszavak létrehozását, az adott operációs rendszeren történő tárolását, és a "feltörési" technikák is előtérbe kerülnek. Szembesülnek a résztvevők továbbá azzal, hogy a nem erős/összetett jelszavak hamar "kipörgethetők" 1. Titkosítási lehetőségek, néhány algoritmus bemutatása 2. Jelszavak feltörésének lehetőségei, néhány alkalmazás (pl.: hydra) bemutatása 3. Szótáralapú, brute force, szabálybázisú támadások 4. Default jelszavak, jelszólisták a Github-on 5. Windows OS, Security Accounts Manager (SAM)
7. alkalom	Hálózati támadások és forgalomeltérítések kerülnek ezen az alkalmon megismertetésre és természetesen bemutatásra. Sniffing, sniffing típusai, spoofing, ARP spoofing, MAC flooding Közbeékelődéses támadás (MiTM) Session támadások fajtái
8. alkalom	Webes támadások nagyon elterjedtek, az "eredmény" szinte azonnal látszik. Ezen és a következő alkalmon megismerik a résztvevők a HTTP alapokat, szerver-kliens architektúrát és áttekintésre kerül természetesen az OWASP módszertan is. 1. Néhány speciális szoftver (pl.: Burp) alkalmazásainak a gyakorlati bemutatása 1.1 Szerveroldali támadások, brute force technikák 1.2 Injection alapú támadások
9. alkalom	Folytatódik a webes sérülékenység- és pentestvizsgálat 1. Szerveroldali támadások, Injection alapú támadások (pl.: Sql) alapjai, RFI, LFI 2. Kliensoldali támadások fajtái (XSS), alapjai
10. alkalom	Méltán népszerű a WiFi (IEEE 802.11) elleni támadások 1. WiFi (IEEE 802.11) alapok, WPA, WPA2, stb 2. Támadási lehetőségek, jelszavak, Beacon flood, Fake AP készítése Szoftverrádió (SDR) alkalmazása
11. alkalom	1. Az IT biztonságban a leggyengébb láncszem mindig a felhasználó. Ezért a résztvevők megismerik a Social Engineering alapjait, például az adathalászatot. 2. Ha a támadók megfertőznek szervereket számítógépeket, akkor azt szeretnék vezérleni a későbbiekben. Ezen az alkalmon megismerjük a C2 szerverek használatának a szükségességét.

12. alkalom	Mi történik egy támadás után? Hagyott-e valami nyomot a támadó, amire következtetni lehet a céljára, a személyére, a támadás sikerességére? Vagy egy rendőrségi lefoglalás után hogyan történik a nyomkeresés? A résztvevők megismerik a Forensics alapjait ezen az alkalmon. 1. Windows forensics alapjai 2. Barangolás a Dark Web-en Számonkérés

SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE / ASSESMENT'S METHOD

Maximálisan 80 pont szerezhető:

- 40 pont az írásbeli teszt alapján

- 40 pont a Python / C / C# nyelven létrehozott alkalmazás és annak dokumentációja alapján

A kurzus sikeres teljesítésének egyik feltétele, hogy a hallgató az írásbeli teszten legalább 60%-ot, azaz legalább 24 pontot érjen el, illetve a létrehozott alkalmazásra és dokumentációjára kapott értékelés is legalább 60%-os eredményű, azaz legalább 24 pontos legyen. A pótlásra/javításra egy lehetőség van.

A kurzus sikeres teljesítésének másik feltétele, hogy a hallgató maximum 3 alkalomról hiányozhat, az első és az utolsó alkalmon a személyes részvétel kötelező.

Ha a fenti két feltétel teljesül, a kurzus teljesítése sikeres, és a kapott 48-80 pont beleszámít az intézményi felvételi pontokba.

Ha a kurzus teljesítése sikertelen, a résztvevő felvételi pontot nem szerezhet.

KÖTELEZŐ IRODALOM / OBLIGATORY MATERIAL

AJÁNLOTT IRODALOM / RECOMMENDED MATERIAL