Izvješće-13.12.2024-SymSpace

Posjet Cyber Rangeu SymSpace

13.12.2024. smo posjetili cyber range koji se nalazi u sklopu vojnog učilišta dr. Franjo Tuđman u Zagrebu.

Na cyber rangeu nam je objašnjeno kako se pokreću, izrađuju i izvršavaju virtualni napadi na simulatoru SymSpace. Iako nismo imali priliku koristiti ili pristupiti simulacijama napada, mogli smo koristiti njihove materijale za učenje koji su vrlo slični HackTheBox (HTB) materijalima. Glavna razlika je u tome što HTB korisnicima pruža više informacija (od kojih su neke i redundantne), dok su SymSpaceovi materijali puno koncizniji i kraći.

Iskustva s Pathovima

VA Analyst Path

U okviru VA Analyst patha riješio sam vježbu *Unsafe deserialization and SSTI (Server-Side Template Injection)*.

Koraci vježbe:

1. **Deserijalizacija kolačića**
   - Počeli smo s jednostavnom deserijalizacijom kolačića.
2. **Deserijalizacija Pickle objekta (Python)**
   - Kreirali smo payload koji otvara reverse shell.
3. **Deserijalizacija Java objekta**
   - Koristili smo alat `ysoserial` za kreiranje payloada koji otvara reverse shell.
   - Prepoznali smo serijalizirani Java objekt po prefiksu `RO0ABX`.
4. **SSTI iskorištavanje**
   - Iskoristili smo znanje iz deserijalizacije kako bismo napravili SSTI na "custom" 404 stranici.

Red Team Operator Path

U ovom pathu sam prošao module koji detaljno pokrivaju *Lockheed Martin kill chain* faze napada:

1. **Reconnaissance**
   - Prikupljanje informacija, što pasivnije to bolje, kako bismo ostali ispod radara.
2. **Weaponization**
   - Kreiranje "oružja" temeljenog na prikupljenim informacijama.
3. **Delivery**
   - Dostavljanje oružja, npr. phishing, fizički mediji, MITM.
4. **Exploitation**
   - Iskorištavanje ranjivosti sustava.

5. **Installation**
    - Omogućavanje postojanosti napadača u sustavu.
6. **Command & Control (C2)**
    - Kontrola i upravljanje sustavom.
7. **Actions on Objective**
    - Izvršavanje ciljanih radnji.

Ova lekcija bila je izrazito teorijska za razliku od praktično orijentiranog VA Analyst patha.

Zaključak

Nakon slušanja o cyber rangeu te sudjelovanja u jednoj teorijskoj i jednoj praktičnoj lekciji, jedva čekam priliku da se vratim. Planiram završiti započete pathove, ali i isprobati simulirane napade jer vjerujem da se kroz njih može najviše naučiti.