Sigurnost operacijskih sustava i aplikacija
Tin Plavec

Laboratorijska vježba 2
Izvještaj

Koraci napada

Potrebno je konstruirati stablo napada. Za početak ćemo raspisati moguće načine na koje bi napadač mogao ostvariti svoj cilj. Svaki korak ima svoj broj koji odgovora poziciji na stablu. Korak 1.1.1. je prvo *dijete* koraka 1.1.

0. Ukradeni podaci o osobi Pero Lokas
Ovo je korijenski čvor, odnosno cilj napada. Ukoliko napadač uspije doći iz nekog od lista do korijenskog čvora, napad je uspješan, a naš sustav kompromitiran.

1. Krađa autentifikacijskih podataka
Ukoliko se napadač domogne lozinke, može se prijaviti u sustav kao Pero Lokas te saznati sve ostale podatke o toj osobi. Dodatno pomaže što je korisničko ime javni podatak.
1.1. Krađa društvenim inženjeringom
1.1.1 Phishing napad (MITRE: https://attack.mitre.org/techniques/T1566/)
Napadač može stvoriti lažnu web stranicu čiji obrazac za prijavu izgleda isto kao i na stvarnoj web stranici. Zatim URL na lažnu web stranicu pošalje ciljanoj osobi koja se pokuša prijaviti na lažnu stranicu čime odaje svoju lozinku.
1.1.2 Impersonacija
Napač se pretvara da je neka osoba s autoritetom ili ugledom, kontaktira ciljanu osobu te dobiva povjerenje te osobe. Zatim smišlja neki razlog da dobije korisnikovu lozinku, a također može ga poslati na lažnu stranicu koja izgleda isto i ima sličnu domenu. Napadač može impersonirati neku nadređenu osobu, policijskog službenika ili pak nekog sigurnosnog eksperta.
1.2. Prisluškivanje prometa ciljane osobe [AND čvor]
1.2.1. Prisluškivanje komunikacije preko HTTP
Promet preko protokola HTTP nije enkriptiran te napadač lako može prisluškivati sav promet pa tako i lozinku koja se šalje u čistom obliku.
1.2.2. Spajanje na istu mrežu kao i ciljana osoba
Napadač se spaja na mrežu koju korisnik koristi kako bi ga mogao prisluškivati. Napadač to može postići jer npr. korisnikov usmjernik koristi zadane postavke. S druge strane, napadač može stvoriti svoju otvorenu mrežu na koju će se korisnik spojiti.
1.3. Krađa sjednice iz preglednika (MITRE: https://attack.mitre.org/techniques/T1539/)
Napač krade od korisnika kolačiće, uključujući i identifikator sjednice pomoću kojeg se moguće autentificirati kao korisnik. Ovo može biti npr. XSS napad.

2. Eskalirane privilegije na web poslužitelju
(MITRE:https://attack.mitre.org/techniques/T1068/)
2.1. Napad na staru inačicu OS-a
Domaćin web poslužitelja koristi zastarjeli operacijski sustav i zastarjele pakete s kritičnim ranjivostima koje napadač može iskoristiti za eskalaciju privilegija.
2.1.1 Skeniranje web poslužitelja
Napadač može skenirati web poslužitelja kako bi saznao inačicu OS-a i kritičnih paketa.
2.2. Eksploatacija ranjivosti u aplikaciji
Aplikacija kao takva može imate kritične ranjivosti pomoću kojih napadač može pristupiti podacima svih korisnika.
2.2.1. SQL ubacivanje (MITRE: https://capec.mitre.org/data/definitions/66.html)
Iako je ovaj napad široko poznat, još uvijek je aktualan.
2.2.2. Iskorištena ranjivost u nekom od *plugina*
Razvojnici aplikacija često koriste vanjske biblioteke i *plugine* kako bi ubrzali razvijanje aplikacije, bez posebne sigurnosne provjere tih programa.
2.2.3. Napad pomoću informacija iz *logova*
Ukoliko aplikacija ne barata dobro s iznimkama i evidentiranjem, napadač ih može iskoristiti za dobivanje informacija o sustavu i neovlašten pristup sustavu,
2.3. Napad na *deployment* okruženje
2.3.1. Iskorištena ranjivost u CI/CD cjevovodu
Napadač dobiva pristup cjevovodu čime dobiva uvid u *deployment* i pristup kritičnim varijablama okruženja.
2.3.2. Upogoniti vlastiti kontejner (MITRE: https://attack.mitre.org/techniques/T1610/)
Napadač upogonjuje maliciozni kontejner s visokim privilegijama koji skida maliciozni program.

3. Kompromitiran *backup* sustav
Sigurnost *backupa* često se previdi, iako je kritična. Uzalud smo osiguravali aplikaciju, ako nam *backup* proces i spremište nisu sigurni.
3.1. Pristup *backup* spremištu [AND čvor]
3.1.1. Iskorištena ranjivost programske podrške *backup* spremišta
Napač iskorištava ranjivost spremišta kako bi pristupio *backup* podacima.
3.1.2. Krađa enkripcijskog ključa
Napač krade ili pogađa loš enkripcijski ključ kako bi mogao dešifrirati *backup* podatke.

Moguće zaštite od napada
1. Vatrozid
Ukoliko se aplikacija koristi interno unutar neke kompanije, poželjno ju je zaštititi vatrozidom.
2. Treniranje zaposlenika
Zaposlenici i korisnici trebali bi proći obuku kako bi bili otporni na napade društvenog inženjeringa.
3. Promjena zadanih postavki
Zadana postavke poput lozinke i vrata uvijek treba promijeniti jer ti podaci su javno poznati.
4. Smanjiti količinu javnih informacija
Korisnička imena su javno dostupno što samo olakšava posao napadaču, a vjerojatno nije potrebno za funkcioniranje aplikacije.

5. Koristiti HTTPS
6. Testirati aplikacijski kod na česte ranjivosti
Ranjivosti SQL ubacivanja i XSS vjerojatno bi bile uspješno detektirane pomoću alata za skeniranje ranjivosti.
7. Uvesti politike *deployment* okruženja
Većina *deployment* okruženja nudi opcije za ograničavanje kontejnera koji se smiju vrtiti u okruženju. Također, moguće je i ograničiti najveća prava koja kontejneri mogu uzeti.

Stablo napada

Stablo ćemo prikazati s korijenskim čvorom na vrhu. Pretpostavlja se da je svaki čvor OR, ako nije drukčije naznačeno (kružnim lukom). Na stablo možemo i dodati mjere zaštite. Za njih ćemo koristiti zelenu boju i drukčiji geometrijski oblik.
Izabrao sam alat ADTool (https://satoss.uni.lu/members/piotr/adtool/) jer je open-source i nudi mogućnost dodavanja mjera zaštite različitom vizualizacijom.

Stablo napada priloženo je u posebnoj datoteci, a ovdje je umanjen prikaz: