IT BIZTONSÁG

4. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

RENDELKEZÉSRE ÁLLÓ IDŐ:

15:00

Ismertető a feladathoz

Fontos információk

A forduló után a megoldások publikálásával együtt iránymutatásként elérhetőek lesznek a **helyezéssel kapcsolatos információk**, látni fogod, hogy a kategóriában a játékosok 20%, 40% vagy 60%-a közé tartozol-e épp.

Felhívjuk figyelmedet, hogy a következő, **5. fordulótól az egyes kategóriák csak a kijelölt napokon lesznek megoldhatóak 7-22 óra között**, érdemes letöltened a naptárat a Kategóriáim menüpontban.

Negyedik forduló

A támadók az egyik webszerverünkön és a mailszerverünkön is lyukat tudtak ütni az exploitjaik segítségével - úgy tűnik nem minden komponens volt teljesen up-to-date a támadás napján, illetve a végpont-védelmünk sem detektálta a támadók összes bevetett eszközét.

A csapattal most az a feladat hárul rátok, hogy kiderítsétek, hogyan és merre mozdultak tovább a támadók a hálózatunkban, miután sikeresen bejutottak a két gyenge pontunkon keresztül.

Felhasznált idő: 02:06/15:00 **Elért pontszám:** 0/23

1. feladat 0/2 pont

Mit jelent a C2 rövidítés?

Válasz

- ○ Control Center

- ◯ Command & Control
- ◯ Command & Conquer
- ◯ Connection Control

Magyarázat

2. feladat 0/2 pont

Az alábbiak közül melyik **NEM** elégséges szempont ahhoz, hogy egy antimalware szoftver egy programot kártékonynak minősítsen?

Válasz

- ◯ a futtatható állomány hash-e
- ◯ IP címek és domainek, ahová a program csatlakozik
- ◯ az állományban található stringek
- ◯ a programfájl neve

Magyarázat

A fájlnév tetszőlegesen bármire átírható bárki által, akár már egy ismert kártevő nevére is - ennek következtében ez nem egy megbízható azonosítási támpont (vírusdefiníció), csak erre támaszkodva túl sok fals pozitív találatot produkálnának az antivírus szoftverek.

3. feladat 0/3 pont

Az alábbi állítás igaz vagy hamis?

A PSExec egy hatékony és csendes módja a hálózaton belüli más gépekre terjedésnek.

Válasz

- ○ igaz
- ◯ hamis

Magyarázat

Bár a PSExec minden kétséget kizárólag hatékony módszer, emellett kifejezetten zajos is - sok nyomot hagy maga után, amiből az egyik legfeltűnőbb az új Windows service és named pipe-ok létrehozása, arról nem beszélve hogy a lemezre is ír.

4. feladat 0/5 pont

Az eseménynapló és a támadók által hátrahagyott fájlok alapján megállapítható, hogy a behatolók a kerberoasting technika segítségével terjedtek tovább az Active Directorynkban. Mely előfeltételek voltak szükségesek a sikeres kerberoasting támadáshoz?

Válaszok

- ☐ A támadónak local administrator joga van
- ☐ A támadó a domain controllerről indítja a támadást
- ☑ A célfiók jelszava gyenge
- ☐ A TGS támogatja az AES titkosítást
- ☑ A célfiók egy service account

Magyarázat

A kerberoasting támadáshoz sem admin jog, sem domain controller hozzáférés nem szükséges - a lényeg, hogy legyen egy service account, dictionary támadással feltörthető gyenge jelszóval. A titkosítás algoritmusát tekintve nem szükséges, hogy az AES a támogatottak között legyen, sőt, ha az AES nem elérhető és csak az RC4 algoritmus használható, még könnyebb is a támadó dolga.

5. feladat 0/3 pont

Az alábbi állítás igaz vagy hamis?

A Metasploit Frameworkhöz tartozó msfvenom tool payload-encoderjei (msfvenom --list encoders) nem antivírus előli rejtőzködésre lettek kitalálva, hatékonyságuk AV-evasion szempontjából ezért alacsony.

Válasz

- ◯ igaz
- ◯ hamis

Magyarázat

Az encoderek főleg a shellcode-ok nemkívánatos karaktereinek (pl. null) kiszűrésére lettek kitalálva. Bár néha működhet egy sok iterációval enkódolt payload egy-egy gyengébb végpont-védelmi megoldásnál, önmagában ezzel az antimalware megoldások többségét nem lehet átejteni.

6. feladat 0/3 pont

A támadóknak sikerült egy admin jogosultságú reverz shellt szerezniük egy Windows géphez a domainunkban. Volt egy jól obfuszkált/titkosított Mimikatz állományuk, amivel sikeresen begyűjtötték a gép összes felhasználói fiókjaihoz tartalmazó hasheket. Melyik Mimikatz parancs segítségével tudták ezt megtenni?

Válasz

- ◯ lsadump::sam
- ◯ sekurlsa::ekeys
- ◯ sekurlsa::credman
- ◯ kerberos::list

Magyarázat

A kerberos::list a Kerberos jegyeket listázza ki, a sekurlsa::ekeys a Kerberos titkosító kulcsokat. A sekurlsa::credman már jobb irány, de az nem felhasználói fiók hasheket ad vissza, hanem alkalmazások elmentett jelszavait. Az lsadump::sam paranccsal lehet az összes jelszóhasht lekérni, amennyiben a támadók a HKLM/SYSTEM és HKLM/SAM registry hive-ok snapshotjait átadják paraméterként: lsadump::sam hklm_system.reg hklm_sam.reg

7. feladat 0/5 pont

Adott az alábbi privát, root userként futó crontab a Linux mailszerverünkön:

```
0 12 */1 * * /usr/bin/find /var/vmail/*/*/Maildir/cur -size +30M -exec /usr/bin/ls -lah {} \; > /root/
```

Alapértelmezett könyvtár- és fájljogosultságok mellett felhasználható-e ez a periodikusan futó parancs egy */var/vmail* könyvtárhoz írási jogosultsággal rendelkező támadó által privilege escalationre, és akár egy root shell megszerzésére?

Válasz

- ○ igen
- ◉ nem

Magyarázat

Bár a crontab összetett és wildcardokat tartalmaz, a futtatott programok abszolút útvonallal vannak megadva, az -exec flagbe pedig nem lehet becsempészni saját binary útvonalat, mivel a wildcardok nem önállóan állnak, hanem egy útvonalhoz kötve. Az ls parancsból "kiszökni" sem lehetséges.