IT BIZTONSÁG

2. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

RENDELKEZÉSRE ÁLLÓ IDŐ:

25:00

Ismertető a feladathoz

Fontos információk

> Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat
>
> A kérdésekre **mindig van helyes válasz**! Ha csak egy helyes válasz van az adott kérdésre, radio button-os választási lehetőségeket fogsz látni.
>
> **Olyan kérdés viszont nincs, amelyre az összes válasz helyes!**

Egyéb információkat a versenyszabályzatban találsz!

A feladatlap elindítása után letölthető csatolmányban egy nyílt forráskódú IPS naplófájljának egy részletét fogod találni.

Indítás előtt bizonyosodj meg róla, hogy használatra készen állnak a kedvenc eszközeid szövegalapú logfájlok elemzéséhez, összesítéséhez!

Második forduló

Sajnos úgy tűnik valóban behatoltak a rendszereinkbe.

Egy gyors triage-olás, eszkaláció és az érintett gépek, hálózatok izolálása után úgy néz ki, sikerült elérni, hogy ne okozzon további károkat a támadás.

A csapatban mindenkit egy közös cél vezérel - kideríteni hogy mi is történt pontosan.

Felhasznált idő: 02:06/25:00 **Elért pontszám:** 0/20

1. feladat 0/5 pont

Az egyik távoli adatközpontunkat is érintette a támadás. Az ottani kollégáknak sikerült időben lekapcsolni az érintett Windows VM-et és elizolálni nekünk vizsgálatra, viszont van egy kis probléma - a virtuális merevlemez image óriási, a sávszélesség illetve a rendelkezésre álló idő pedig véges. A kollégák felrakták nekünk egy SMB share-re a VHD fájlt - van valamilyen módja a távoli VHD fájlban való egyszerű és gyors böngészésnek Linux eszközünkről anélkül, hogy az egészet le kellene töltenünk?

Az ottani kollégák a VHD fájlt a következő útvonalra helyezték el nekünk:

//share.cryptador.io/internal/Images/2021-10-14/e8bd75f4-acbd-458f-a902-801eda8fa75f.vhd

Válasz

- ( ) Nincs ilyen módja, le kell tölteni az egészet
- ( )
```
$ mount -t cifs //share.cryptador.io/internal /mnt/remotesmb -o rw && guestmount --add /mnt/remot
```
- ( )
```
$ mount -t ntfs //share.cryptador.io/internal /mnt/remotesmb -o rw && guestmount --add /mnt/remot
```
- ( )
```
$ mount -t cifs //share.cryptador.io/internal /mnt/remotesmb -o rw -f && guestmount --add /mnt/re
```

Magyarázat

Mivel az SMB share-k fájlrendszere CIFS típusú, ezért a mount parancsot arra a típusra kell hívni, nem NTFS-re. A -f flaget tartalmazó mount parancs nem fogja ténylegesen mountolni az SMB könyvtárat, csak szimulálja azt (az -f a --fake flag rövidítése).

2. feladat 0/3 pont

Egyik Linux szerverünkön végpont-védelemnek ClamAV-t használunk.

Hogyan tudjuk gyorsan kilistázni a daemon által eddig megtalált kártevőket minél régebbre visszamenőleg?

Válasz

```
$ clamscan --log -i
```

```
$ zgrep FOUND /var/log/clamav/clamav.log*
```

```
$ grep -r detect /var/log/clamav
```

```
$ ls -la ~/.clamav/viruses
```

Magyarázat

A default ClamAV daemon korábbi futásainak logjai a /var/log/clamav könyvtár alatt találhatóak, tehát csak itt érdemes keresni. A pozitív találatot FOUND kulcsszóval jelölik a logok. A zgrep és a wildcard segítségével a régebbi, már "archivált", gzippelt logfájlokat is át tudjuk kutatni találatokért.

3. feladat 0/3 pont

A tűzfalunk az alábbi parancssal volt beállítva:

```
$ iptables -A INPUT -p tcp -j LOG --log-tcp-options
```

A logokból úgy fest, hogy 2 nappal a támadás előtt portscannelték az egész hálózatunk IP tartományát. Az alábbi releváns sort találtuk a logokban:

```
Oct 12 17:36:48 cryptador-web2 kernel: [373506.660353] DROP IN=eth0 OUT= MAC=3c:f7:64:18:cd:60:96:fb:9
```

Mely portscanner parancs(ok) hatására keletkezhetett a fentihez hasonló sor a logban?

Válaszok

- [ ] nmap -sT 10.10.0.10/30

- [x] zmap -p 22 10.10.10.0/24
- [x] masscan -p 20-9001 10.10.10.0/28
- [ ] nmap -p 21,25,80 10.10.10.10

Magyarázat

Az -sT flages nmap parancsnál a megadott CIDR tartomány (10.10.0.8 - 10.10.0.11) nem fedi le a célpont IP címét (DST=10.10.10.10).

A másik nmap parancs esetében pedig a célpont szkennelt portja (DPT=22) nincs jelen a felsoroltak között.

4. feladat 0/2 pont

Az alábbi állítás igaz vagy hamis?

A non-volatile adat értékesebb, mint a volatile adat, ezért elsősorban arra kell fókuszálni incident response során.

Válasz

- ( ) igaz
- (•) hamis

Magyarázat

Bár mindkét adatfajta nagyon értékes egy cybersecurity incidens kivizsgálása esetén, a volatile adat (pl. aktuális rendszermemória tartalma) sokkal több nyomot rejthet a támadó módszereivel kapcsolatban. Manapság a legtöbb támadó igyekszik teljesen in-memory dolgozni anélkül, hogy bármit a lemezre írnának, így jelentősen kevesebb kézzelfogható non-volatile bizonyítékot hagyva a támadásról.

5. feladat 0/2 pont

Volatility Framework segítségével szeretnénk áttúrni egy Windows 10 gép memory image-ét. Azt a fülest kaptuk, hogy a snapshot készítésekor még volt aktív kapcsolat a támadó gépe és az érintett eszköz között. Melyik plugint futtatva kaphatunk több információt a támadóról?

Válasz

- mac_network_conns
- connections
- netscan
- sessions

Magyarázat

Csak a connections és a netscan pluginok adnak vissza Windows gépről hálózati kapcsolatinfókat. A connections plugin csak Windows XP és Server 2003 rendszerek snapshotjain működik, így egyedül a netscan marad helyes megoldásként.

6. feladat 0/0 pont

Egy privát tárhelyként szolgáló gépünkön az alábbi iptables paranccsal engedélyeztük csak egyetlen IP címnek (81.96.128.91) a kívülről beérkező FTP forgalmat:

```
iptables -I INPUT -p tcp ! -s 81.96.128.91 --dport 21 -j DROP
```

Sikerült-e bármilyen kívülről érkező FTP-csatlakozást blokkolni így, az engedélyezett cím kivételével?

Válasz

- igen
- nem

Magyarázat

Update: a feladatot a versenyzői visszajelzések alapján kivettük az értékelésből, ugyanis a megfogalmzás félreérthető lehet, és nem lehet ebből az egy tűzfalszabályból egyértelműen következtetni a helyességre.

IPv6 protokollon keresztül, az IPv6 címünk ismeretében továbbra is szabadon bárki csatlakozhatott a szerverünk FTP portjához. Ahhoz, hogy ott is letiltsuk az összes portra érkező kapcsolódást, ugyanezt a parancsot az ip6tables-zel is le kellett volna futtatni.

7. feladat 0/5 pont

A letölthető csatolmányban található egy fail2ban log, amely rögzítette a bejelentkezési kísérleteket a mailszerverünkön egészen a megerősített támadás napjáig. Gyanakszunk, hogy a támadó IP címe köztük lehet - korábban biztosan megpróbált bejelentkezni ssh-n keresztül egy megszerzett jelszó birtokában.

Mely IP cím lett a legtöbbször bannolva a logfájl szerint?

Válaszok

A helyes válasz:
171.225.185.69, 198.98.52.69, 199.195.254.38
198.98.52.69
171.225.185.69
199.195.254.38, 198.98.52.69, 171.225.185.69
199.195.254.38
171.225.185.69 198.98.52.69 199.195.254.38
6x lett mind: 171.225.185.69 198.98.52.69 199.195.254.38
198.98.52.69, 199.195.254.38, 171.225.185.69
199.195.254.38

Magyarázat

A logból tetszőleges szövegfeldolgozó módszerrel relatíve gyorsan ki lehet hámozni a szükséges információt.

A legtöbb Linux installáción remek parancssori eszközök állnak rendelkezésre, amelyek az ilyen logokat fel tudják dolgozni. Az egyik ilyen parancs-lánc lehet akár a következő:

```
$ grep 'Ban' fail2ban.log | tr -s ' ' | cut -d' ' -f8 | sort | uniq -c | sort
```

De awk segítségével is meg lehet oldani a dolgot:

```
$ awk '($(NF-1) = /Ban/){print $NF}' fail2ban.log | sort | uniq -c | sort -n
```

Akármelyik parancsot lefuttatva látszik, hogy 6 a legtöbb tiltások száma, és ez három IP címre is illik: 199.195.254.38, 198.98.52.69, 171.225.185.69.

Megjelenés

Világos