IT BIZTONSÁG

1. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

RENDELKEZÉSRE ÁLLÓ IDŐ:

10:00

Ismertető a feladathoz

Fontos információk:

A kérdésekre **mindig van helyes válasz**! Ha csak egy helyes válasz van az adott kérdésre, radio button-os választási lehetőségeket fogsz látni.

Kérjük, hogy a feladatok szövegeit **ne másold** és a böngésződ fejlesztő eszközét/ konzolját se nyisd meg feladatmegoldás közben! Mindkettő kizárást vonhat maga után.

Minden forduló után a **megoldások csütörtök reggel 8 órakor** lesznek elérhetőek.

A megoldásokkal kapcsolatos esetleges **észrevételeket a megoldások megjelenését követő kedd éjfélig** várjuk.

A több válaszlehetőségű feleletválasztós kérdéseknél járnak **részpontszámok, ha egyik rossz választ sem jelölöd be**.

Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat.

Minden feladatsornak van egy **becsült minimum megoldási ideje** (legalább a feladat elolvasási ideje). Aki ennél rövidebb idő alatt oldja meg, kizárható a versenyből.

Az első kategória után, amelynek a feladatlapját megoldod a fordulóban, kapni fogsz egy 2-3 perc alatt kitölthető **kérdőívet**. Az ezekből összeállított piackutatás legfontosabb eredményeit a díjátadót követően Veled is megosztjuk majd. Formáljuk közösen a piacot!

Első forduló

Egy nyugodt napnak indult a mai is. A reggeli kávé illata betöltötte a Cryptador Solutions irodáját, a kollégák félálmosan ültek le az asztalukhoz. A szunyókás reggeli idillt viszont gyorsan megtörték az egyre erősödő, aggódó hangok - szokatlan forgalmat, különös fájlokat véltek kollégák felfedezni az infrastruktúránkban.

Alighogy összeraktad mi is történik körülötted pontosan, már érkezik is fentről a hívás, hogy támadásgyanú áll fent és mihamarabbi kivizsgálást szeretne a főnököd.

Az incident response csapat vezetőjeként felvetted hát a kedvenc hacker-sapkád, és a csapatoddal belevágtál a kutatásba...

1. feladat 0/1 pont

Mit jelent az IDS rövidítés?

Válasz

- Internet Deanonymizing Service
- Identifiable Data Synchronization
- Intrusion Detection System
- Interconnected Device Storage

Magyarázat

2. feladat 0/2 pont

Mi a különbség a Network-based IDS (NIDS) és a Host-based IDS (HIDS) között?

Válasz

- A NIDS a belső hálózat és az internet közötti forgalmat, míg a HIDS a belső hálózat összes tagja közötti forgalmat ellenőrzi
- A NIDS az általános hálózati forgalmat, míg a HIDS az egyéni eszközök viselkedését, műveleteit vizsgálja
- A NIDS kizárólag központi (pl. domain controller, Kerberos szerver) eszközöket vizsgál, minden egyéb gépért a HIDS felel
- Csupán a telepítés helyszínében különböznek, a funkciójuk és működésük megegyezik

Magyarázat

3. feladat 0/5 pont

Mely logokat érdemes áttekinteni egy Linux webszerveren támadásgyanú esetén, ha tudjuk, hogy a támadó nem szerzett root jogot a gépen?

Válaszok

- [ ] /var/log/dpkg.log
- [x] /var/log/apache2/error.log
- [ ] /var/log/letsencrypt/letsencrypt.log
- [x] /var/log/syslog

Magyarázat

A webszerver hibalogja és a syslog tartalmazzák a leginkább releváns nyomokat egy behatolás esetén. Az errorlog tartalmazhat próbálkozásokat a támadó részéről a sikeres parancs futtatása előttről, míg a syslogban potenciálisan megtalálhatóak a nyomai egy shell elindításának, miután a támadó kódot tudott futtatni a szerveren.

A letsencrypt log a weboldalak SSL-tanúsítványainak megújításáról tartalmaz infókat - a támadó nagy valószínűséggel ezzel nem foglalkozik, főleg hogy ehhez root jogot is kellene szereznie előtte. A dpkg log a packagekkel történt változásokat rögzíti, a root jog szükségessége miatt ezt is ki lehet zárni.

4. feladat 0/2 pont

Az alábbiak közül melyik jelenség utalhat a **legkevésbé** egy sikeres behatolásra?

Válaszok

- [ ] Megnövekedett kimenő hálózati forgalom
- [ ] Módosult végpont-védelem kivétellista
- [x] Magasabb memória, CPU és lemez IO használat
- [x] Átlagosnál több rendszerújraindulás

Magyarázat

A felsorolt "tünetek" közül a gyakori teljes újraindulás a legzajosabb és legészrevehetőbb jelenség, és ezt a támadók is igyekeznek annyira aktívan elkerülni, amennyire csak lehet.

5. feladat 0/2 pont

A Windows Eseménynaplóban az utóbbi időben jelentősen felszaporodtak a 4672-es azonosítójú események. Utalhat-e ez sikeres behatolásra?

Válasz

- ◯ igen
- ◯ nem

Magyarázat

A 4672-es event ID a sikeres adminisztrációs fiókokba történő bejelentkezést jelöli. Amennyiben ezek feltűnően megsokszorozódtak az utóbbi időben, lehetséges, hogy egy támadónak sikerült egy admin fiók jelszavához vagy NTLM hashéhez jutnia, és azt felhasználva lépeget be a hálózatba.

6. feladat 0/2 pont

Hálózatunkon megszaparodtak a kifelé történő pingelések (ICMP echo request). Utalhat-e ez sikeres behatolásra?

Válasz

- ◯ igen
- ◯ nem

Magyarázat

Végső megoldásként az ICMP/ping csomagokat is lehet adat exfiltrálására használni a DNS-hez hasonlóan, ha esetleg a tűzfalak az összes kifelé menő kapcsolatot tiltják. Az ICMP ECHO csomagok tartalmazhatnak tetszőleges adatot, ezt kihasználva lehet a csomagokban adatot "átcsempészni" a tűzfalon.

https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-icmp-tunneling-to-own-your-network/

7. feladat 0/2 pont

Alapesetben hol találhatóak az iptables logok Debian-alapú rendszereken?

Válasz

- [ ] /var/log/iptables.log
- [x] /var/log/kern.log
- [ ] /var/log/fail2ban.log
- [ ] /var/log/dmesg

Magyarázat

Az iptables logok mindig kernelüzenetként kerülnek logolásra, ezért vagy a /var/log/kern.log vagy a /var/log/syslog útvonalak alatt találhatóak egy default Debian-alapú rendszeren.