Zadanie 5 (Sieťová bezpečnosť)

November 11, 2024

Cieľom zadania je oboznámiť sa s analýzou sieťových logov a skúmaním rôznych bezpečnostných incidentov. Zadanie je zložené z dvoch menších častí a k dispozícii budete mať nasledujúce súbory:

1. **Časť 1**:
   (a) `auth.log` - jedná sa o približne 20 minút logov z `sshd` servisu. Tento servis predstavuje bežiaci *OpenSSH* server, ktorý prijíma spojenia prostredníctvom SSH protokolu.
   (b) `wtmp.txt` - jedná sa o výpis z `var/log/wtmp` logu, ktorý obsahuje informácie o prihláseniach/odhláseniach v systéme.
2. **Časť 2**:
   (a) `output.pcapng` - PCAP súbor zachytávajúci sieťovú prevádzku na systéme.

Úlohy:

1. **Časť 1.** V rámci tejto časti vyšetrujete *brute-force* útok na SSH. Prostredníctvom forenznej analýzy súborov `auth.log` a `wtmp.txt` vyriešte nasledujúce úlohy:
   (a) Z akej IP adresy prebiehal útok (t.j. IP adresa útočníka)?
   (b) Ako sa volal používateľ v napadnutom systéme, ku ktorému získal útočník po prelomení prístup?
   (c) V akom časovom bode sa podarilo útočníkovi prihlásiť na zraniteľný server?
   (d) Všetky úspešné SSH pripojenia majú priradené svoje *session-id*. Aké *session-id* bolo priradené útočníkovi, keď sa prihlásil prostredníctvom mena používateľa z otázky b)?
   (e) Po úspešnom prihlásení následne útočník pridal nového používateľa do systému a nastavil pre neho vyššie oprávnenia. Ako sa volal tento pridaný používateľ?

(f) Po vytvorení nového používateľa sa útočník následne prihlásil (otázka e)) a využil jeho oprávnenia na stiahnutie súboru z webu. Napíšte celý príkaz aj s cestou k tomuto súboru.

(g) Ako dlho trvala prvá útočnikova *session*? Výsledok napíšte v sekundách (pomôžte si odpoveďou na otázku c)).

2. **Časť 2:** V rámci tejto časti budete vyšetrovať útočníkovu aktivitu na serveri, počas ktorej nainštaloval tzv. *reverse shell* [1]. Na čítanie PCAP súboru môžete využiť štandardný nástroj na analýzu sieťovej prevádzky, *Wireshark* [2]. Vyriešte nasledujúce úlohy:

   (a) Aké percento paketov v sieťovej prevádzke používa protokol TCP?

   (b) Aká je útočníkova IP adresa?

   (c) Napíšte celú cestu k súboru (na zraniteľnom serveri) kde útočník prekopíroval škodlivý súbor.

   (d) Aký port použil útočník pri získaní *reverse shellu*, ktorým sa pripája zo zraniteľného servera?

   (e) Po získaní prístupu spustí útočník na serveri niekoľko príkazov. Identifikujte spustené príkazy a identifikujte príkaz, ktorým sa útočník pokúša uložiť súbor na serveri (prípadne aj dešifrovať názov).

   Poznámka: žiadne IP adresy z logov nie je nutné skenovať. Na riešenie zadania stačí iba samotná analýza logov.

Deadline zadania je **26.11.2024** o **13:37**. Zadanie sa odovzdáva do **akademického informačného systému** (AIS) do zvoleného miesta odovzdania. Odovzdáva sa dokumentácia vo formáte **PDF** (!!!). Odovzdáva **jeden** člen z tímu.

Literatúra

[1] What is a reverse shell? `https://www.imperva.com/learn/application-security/reverse-shell/`.

[2] Wireshark. `https://www.wireshark.org/`.