Testy Penetracyjne

Analiza skanów podatności

Arkadiusz Chrobot

Katedra Systemów Informatycznych

10 kwietnia 2024

Plan

Wstęp

Skanowanie podatności może dostarczać dużej ilości informacji. Jej analiza jest kluczowa dla efektywności kolejnych faz testów penetracyjnych. Celem jest wytypowanie luk, które mogą być najbardziej przydatne do eksploatacji badanego systemu informatycznego. Dla zespołu zajmującego się cyberbezpieczeństwem analizowanie wyników skanowania pozwala określić kolejność, w jakiej powinny być naprawiane podatności.
Typowy opis luki zabezpieczeń, w raporcie wygenerowanym przez skaner podatności, zawiera jej nazwę, informację o jej istotności (mała, średnia, wysoka, krytyczna), szczegółowe dane na jej temat, wskazówki jak ją usunąć, odnośniki do źródeł danych oraz ocenę ryzyka.

Interpretacja CVSS

Istotność (ang. *severity*) podatności jest najczęściej wyliczana przy pomocy *Common Vulnerability Scoring System* (▸ CVSS). Dodatkowo, niektóre narzędzia umieszczają w opisie luki jej *wektor* CVSS. Najnowszą wersją tego systemu oceny podatności jest ▸ 4.0, wprowadzona w 2022 roku. Jednakże nie została ona wprowadzona jeszcze do wszystkich narzędzi, a sposób wyliczania z jej użyciem istotności luki jest dosyć zawiły. Na wykładzie zostanie przedstawiona wersja ▸ 3.0 tego systemu.

Interpretacja CVSS

Przykładowy wektor CVSS może być następujący:

`CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N`

Początek wskazuje wersję CVSS, które została użyta do określenia tego wektora. Litery `AV` są skrótem od angielskich słów *attack vector*, oznaczających wektor ataku. Ta metryka może przyjmować następujące wartości opisowe i numeryczne:

Physical (P) — 0.2 Intruz musi mieć fizyczny dostęp do urządzenia z podatnością.

Local (L) — 0.55 Intruz musi mieć fizyczny lub logiczny dostęp do systemu z podatnością.

Adjacent Network (A) — 0.62 Intruz musi mieć dostęp do lokalnej sieci, do której jest podłączony system z podatnością.

Network (N) — 0.85 Intruz może wykorzystać podatność zdalnie, przez sieć.

Interpretacja CVSS

Litery `AC` oznaczają *złożoność ataku* (ang. *attack complexity*), która może przyjmować następujące wartości:

High (H) — 0.44 Wykorzystanie luki wymaga określonych warunków, które mogą być trudne do osiągnięcia.

Low (L) — 0.77 Wykorzystanie luki nie wymaga wystąpienia szczególnych warunków.

Z kolei `PR` oznacza *wymagane uprawnienia* (ang. *required privileges*), metrykę przyjmującą następujące wartości:

High (H) — 0.270 lub 0.50, jeśli *Zasięg* ma wartość *Changed* Intruz musi mieć uprawnienia administratora.

Low (L) — 0.62 lub 0.68, jeśli *Zasięg* ma wartość *Changed* Intruz musi mieć podstawowe uprawnienia.

None (N) — 0.85 Intruz nie musi się uwierzytelniać.

Interpretacja CVSS

Litery `UI` w wektorze CVSS oznaczają *user interaction*, czyli metrykę wskazującą, czy wykorzystanie luki wymaga interakcji z użytkownikiem atakowanego systemu. Może ona przyjmować dwie wartości:

None (N) — 0.85 Do wykorzystania luki nie jest konieczna dobrowolna lub wymuszona pomoc użytkownika atakowanego systemu.

Required (R) — 0.62 Do wykorzystania luki jest konieczna dobrowolna lub wymuszona pomoc użytkownika atakowanego systemu.

Interpretacja CVSS

Litera `S` oznacza z kolei *zasięg* (ang. *scope*), który określa, czy podatność może wpłynąć na komponenty systemu poza jej miejscem występowania. Ta metryka może przyjmować następujące wartości:

Unchanged (U) Wykorzystanie podatności może wpłynąć jedynie na zasoby podlegające mechanizmowi bezpieczeństwa (ang. *security authority*), w którym występuje luka.

Changed (C) Wykorzystanie podatności może wpłynąć na zasoby znajdujące się poza jurysdykcją mechanizmu bezpieczeństwa (ang. *security authority*), w którym występuje luka.

Interpretacja CVSS

Litery C, I i A na końcu wektora CVSS odpowiadają literom w triadzie CIA, czyli oznaczają *poufność* (ang. *confidentiality*), *integralność* (ang. *integrity*) i *dostępność* (ang. *availability*). Mogą one przyjmować następujące wartości:

None (N) — 0.00 Wykorzystanie luki nie ma wpływu na poufność/integralność/dostępność.

Low (L) — 0.22 Dostęp/modyfikacja danych jest możliwa, ale intruz nie ma kontroli nad tym które dane są ujawnione/zmodyfikowane. Wydajność systemu jest obniżona.

High (H) — 0.56 Intruz ma pełny dostęp do danych/może w pełni je modyfikować/może wyłączyć system.

Interpretacja CVSS

Uzyskanie *podstawowej oceny* CVSS (ang. CVSS *base score*), która określa istotność luki, wymaga obliczenia *pod-wyniku oddziaływania* (ang. *impact sub-score*), *wyniku oddziaływania* (ang. *impact score*) i *oceny możliwości eksploatacji* (ang. *exploitability score*). Pierwszą wartość otrzymuje się z następującego wzoru:

$$ISS = 1 - [(1 - Confidentiality) \times (1 - Integrity) \times (1 - Availability)]$$

Drugą uzyskuje się mnożąc *pod-wynik oddziaływania* przez $6,42$, jeśli zasięg (ang. *scope*) jest niezmieniony (ang. *unchanged*). W przeciwnym przypadku stosuje się wzór:

$$Impact = 7,52 \times (ISS - 0,029) - 3,25 \times (ISS - 0,02)^{15}$$

Ocenę możliwości eksploatacji uzyskuje się ze wzoru:

$$Exploitability = 8,22 \times AV \times AC \times PR \times UI$$

Interpretacja CVSS

Ocena podstawowa CVSS jest uzyskiwana według następującego algorytmu:

1. Jeśli *wynik oddziaływania* wynosi 0, to *ocena podstawowa* CVSS też wynosi 0.
2. Jeśli *zasięg* jest *niezmieniony*, to *ocena podstawowa* CVSS jest sumą *wyniku oddziaływania* i *oceny możliwości eksploatacji*.
3. Jeśli *zasięg* jest *zmieniony*, to sumę z poprzedniego punktu należy pomnożyć przez $1,08$.
4. Jeśli wynik przekracza 10, to należy go obniżyć do 10.

Interpretacja CVSS

Ocenę opisową istotności podatności uzyskuje się na podstawie zamieszczonej tabeli.

Wynik CVSS	**Ocena opisowa**
0,0	None
0,1 – 3,9	Low
4,0 – 6,8	Medium
7,0 – 8,9	High
9,0 – 10.0	Critical

Ocena wyników skanowania

Skanery podatności mogą informować o istnieniu podatności w systemie, która w rzeczywistości w nim nie występuje. Takie zjawisko nazywa się *wynikiem fałszywie dodatnim*. W przypadku wątpliwości zespoły zajmujące się cyberbezpieczeństwem mogą zweryfikować wynik bezpośrednio, sprawdzając, czy zostały zainstalowane poprawki lub wręcz symulując eksploatację luki. Czasem może to wymagać konsultacji z innymi pracownikami firmy. Testerzy penetracyjni uzyskują potwierdzenie istnienia podatności, jeśli udaje się ją wykorzystać w trakcie testowania.

Usuwanie podatności jest zazwyczaj działaniem podlegającym kompromisom. Niekiedy osoby odpowiedzialne pracę systemów decydują na przykład o pozostawieniu w użyciu komponentów, które są już niewspierane i mogą zawierać potencjalne luki. Może to mieć związek z koniecznością zachowania kompatybilności z innymi systemami. Takie decyzje powinny być dobrze udokumentowane i uwzględnione w konfiguracji skanerów podatności. Należy jednak wziąć pod uwagę, że mogą naruszać wymogi nakładane przez standardy.

Ocena wyników skanowania

Dosyć często dużą część raportów ze skanów podatności zajmują informację nieformalne, nie mające klasyfikacji opartej na CVSS. Pentesterzy powinni w pierwszej kolejności brać pod uwagę luki o wysokiej i krytycznej istotności. Te nieformalne mogą stanowić podstawę dla dalszego rekonesansu, ale zazwyczaj nie mogą być bezpośrednio wykorzystane do uzyskania dostępu do badanego systemu. Z kolei zespoły d.s. cyberbezpieczeństwa powinny posiadać formalną politykę obsługi takich zgłoszeń, jeśli powtarzają się w kolejnych skanowaniach. Najczęściej sprowadza się ona do uzasadnienia dlaczego dany wynik nie stanowi podstaw do dalszego działania.
Testerzy penetracyjni powinni porównać wyniki skanowania z innymi źródłami informacji o systemie, jeśli są one dla nich dostępne. Takimi źródłami są dzienniki zdarzeń (logi) serwerów, systemy SIEM (ang.*Security Information and Event Management*) oraz systemy zarządzania konfiguracjami.

Ocena wyników skanowania

Niektóre narzędzia do skanowania podatności oferują porównanie bieżących wyników z historycznymi i analizę trendów, takich jak przyrost nowych podatności, wiek wcześniej wykrytych i czas potrzebny do ich naprawy. Te informacje mogą być szczególnie potrzebne dla członków zespołów d.s. cyberbezpieczeństwa.

Często spotykane podatności

Serwery i punkty końcowe

Nawet skanery podatności, których dane o lukach są aktualne, zwykle raportują o problemach, które należą do jednej z kilku „popularnych" kategorii. Jeśli weźmiemy pod uwagę serwery i punkty końcowe (ang. *endpoints*), to najczęściej pojawiającymi się problemami okażą się: brak instalacji poprawek bezpieczeństwa, niewspierane systemy operacyjne i aplikacje, luki przepełnienia bufora (ang. *buffer overflows*), eskalacji uprawnień (ang. *privilege escalation*) — np. *Dirty Cow* — (zdalnego) wykonania dowolnego kodu (ang. *(remote) arbitrary code execution*), luki w firmware, podatności typu Spectre i Meltdown, użycie niebezpiecznych protokołów (np. Telent, FTP), pozostawiony włączony tryb debugowania na środowiskach produkcyjnych.

Często spotykane podatności

Serwery i punkty końcowe

Warto zwrócić uwagę, że do punktów końcowych zaliczane są urządzenia mobilne, które nie zawsze pojawiają się w raportach skanowania bezpieczeństwa, z uwagi na swoje przeznaczenie. Osoby odpowiedzialne za bezpieczeństwo infrastruktury, która zawiera tego typu punkty końcowe powinny skorzystać z usług zarządzania urządzeniami przenośnymi (ang. *Mobile Device Management* — MDM), które pozwalają na ich spójną konfigurację, automatyczne instalowanie poprawek, wymuszanie szyfrowania, zdalne usuwanie danych i ograniczanie instalowania aplikacji.
Inną ważną kategorią punktów końcowych są terminale płatnicze (ang. *point-of-sale* — POS), które podlegają wymaganiom standardu PCI DSS, a mogą zawierać te same podatności jak inne systemy.

Często spotykane podatności

Sieć

Problemy związane z siecią, które mogą wskazać skanery podatności mogą być podobne jak w przypadku serwerów i punktów końcowych (np. nieaktualny firmware), ale także swoiste dla zagadnień sieciowych, np. przestarzałe wersje SSL/TLS, możliwość użycia słabego szyfrowania, problemy z certyfikatami (niezgodność nazw, wygasłe certyfikaty, nieznane centrum certyfikacji (ang. *certification authority*)).
Usługi DNS mogą być traktowane jako osobne źródło podatności. Przykładem może być luka *wzmacniania* DNS (ang. DNS *amplification*). Intruz może ją wykorzystać wysyłając do serwera DNS żądanie, które zawiera podszyty (ang. *spoofed*) adres IP i jest tak skonstruowane, że serwer odsyła pod ten adres odpowiedź o dużym rozmiarze. Jeśli to żądanie trafi do wielu serwerów DNS, to może zablokować (ang. *denial of service*) ofiarę.

Często spotykane podatności

Sieć

Częstym problemem jest również ujawnienie prywatnego adresu IP. Jest on spotykany w przypadku np. źle skonfigurowanych serwerów HTTP, które umieszczają taki adres w nagłówkach odpowiedzi. Podobne problemy, jak w przypadku SSL/TLS mogą wystąpić z wirtualnymi prywatnymi sieciami (ang. *Virtual Private Network* — VPN), np. możliwość użycia słabego szyfrowania. Dodatkowo w przypadku tych rozwiązań problemem może być także nieaktualne oprogramowanie.

Często spotykane podatności

Maszyny Wirtualne

Wiele centrów danych używa maszyn wirtualnych obsługiwanych przez hipernadzorcę typu pierwszego. Z kolei punkty końcowe mogą stosować maszyny wirtualne pracujące pod kontrolą hipernadzorcy typu drugiego. Najpoważniejszymi lukami jakie można spotkać w tych rozwiązaniach są podatności umożliwiające intruzowi ucieczkę z maszyny wirtualnej (ang. *virtual machine escape*), czyli nieuprawnione uzyskanie dostępu do zasobów innej maszyny wirtualnej. Inną istotną kwestią jest dostęp do interfejsu oprogramowania zarządzającego, który powinien być ograniczony, najlepiej tylko do sieci wewnętrznej. Poza tym w środowiskach z wirtualizacją występują podobne lub te same problemy, co w tych które nie stosują tej techniki: zarówno systemy operacyjne-gospodarze (ang. *host* OS), jak i systemy operacyjne-goście (ang. *guest* OS) mogą być nieaktualne, albo mogą pojawić się problemy z bezpieczeństwem na poziomie wirtualnej infrastruktury sieciowej.

Często spotykane podatności

Internet Rzeczy

Internet Rzeczy (ang. *Internet of Things* —IoT), szczególnie w połączeniu z systemami automatyki przemysłowej, takimi jak SCADA (ang. *Supervisory Control and Data Acquisition*) lub ICSs (ang. *Industrial Control Systems*) może być szczególnie trudnym pod względem ochrony rozwiązaniem. Często producenci tego typu rozwiązań nie oferują automatycznej aktualizacji oprogramowania lub w ogóle jej nie oferują. Cześć z urządzeń IoT, to rozwiązania z dziedziny automatyki przemysłowej, które nie były do początku projektowane z myślą o podłączeniu do Internetu i w związku z tym nie mają możliwości aktualizowania systemu operacyjnego i aplikacji. To może dotyczyć także nowszych rozwiązań, które tworzone są jako wbudowane systemy (ang. *embeded systems*).

Często spotykane podatności

Aplikacje Internetowe

Oprócz systemów operacyjnych również aplikacje, w szczególności aplikacje internetowe mogą zawierać podatności interesujące z punktu widzenia testerów penetracyjnych. Wśród nich są luki pozwalające na wstrzyknięcie kodu (SQL Injection, XSS, OS Command Injection), sfałszowanie żądania (CSRF) lub inne (np. XXE).

Pytania

?

Koniec

Dziękuję Państwu za uwagę!