Akademia Handlowa Nauk Stosowanych w Radomiu

Bezpieczeństwo systemów komputerowych Laboratorium 4

Radom 2021/2022

1. Cel zadania

Częstym problemem w zabezpieczeniach systemu komputerowego jest nieodpowiednia znajomość możliwości jego konfiguracji oraz błędy podczas wdrażania określonego rozwiązania. Efektem wymienionych problemów mogą być podatności na określone wektory ataku. Projektant systemu komputerowego powinien w pierwszej kolejności dokonać testów i symulowanych ataków swojego rozwiązania by mieć odpowiednią wiedzę, dla których konfiguracji środowiska należy dokonać korekt.

2. Potrzebne narzędzia.

- kompletny zestaw komputerowy
- system Linux, jednak preferowane będą dystrybucje: Kali Linux, Black Arch, Pentoo Linux (lub równoważne)

LUB

- kompletny zestaw komputerowy z dowolnym system operacyjnym
- oprogramowanie do wirtualizacji (VMWare, Hyper-B, VirtualBox, kvm)
- system Linux jak wskazano wcześniej

3. Informacje wstępne

Zapewnienie bezpieczeństwa rozwiązaniom informatycznym stanowi coraz większe wyzwanie. Obecnie ewentualne defekty konfiguracji oraz nieodpowiednie dysponowanie zasobami systemów komputerowych może spowodować w najlepszym wypadku utratę mało ważnych plików, a w najgorszym nawet przestój linii produkcyjnej, wypłynięcie tajnych dokumentów lub utratę kontroli nad kluczowymi systemami informacyjnymi czy wojskowymi.
Niezależnie od ostatecznego zastosowania tworzonego rozwiązania informatycznego architekt powinien rozpoznać i dokonać zabezpieczeń krytycznych punktów takiego rozwiązania. W przypadku popularnych obecnie systemów rozproszonych elementarnym niebezpieczeństwem będzie połączenie sieciowe pomiędzy ich poszczególnymi punktami końcowymi. Tutaj samo medium, będące najczęściej rozwiązaniem bezprzewodowym, stanowi dość poważną lukę bezpieczeństwa (z technologicznego punktu widzenia). Kolejny problem stanowią protokoły komunikacyjne, których podatności są znane i dobrze udokumentowane, jednak ze względu na skomplikowany proces eliminacji (konieczność zmiany oprogramowania na wszystkich urządzeniach transmisyjnych) są niemożliwe do wyeliminowania w prosty sposób - ich neutralizacja przeważnie musi być wdrożona w protokołach warstw wyższych, w tym w warstwie aplikacji.
Sam poziom zabezpieczeń wdrażanego systemu komputerowego musi zależeć przede wszystkim od:

- ostatecznego celu systemu komputerowego – podejmowane środki muszą być adekwatne do ważkości celu całego projektu (inne będzie dla systemu PC, inne dla inteligentnego domu, a jeszcze inne do autonomicznych systemów produkcji czy autonomicznego nadzoru transportu)
- skomplikowania zadania – im wyższy poziom wdrażanego zabezpieczenia, tym jego skomplikowanie wzrasta. Złożoność zaś ma bezpośrednie przełożenie na efektywność systemu - zarówno pod kątem szybkości transferu danych (dodatkowy narzut przez szyfrowanie - większa ilość potencjalnych powtórzeń spowodowanych błędnym transferem danych), jak i zmniejszenia możliwości obliczeniowych układu (dodatkowe obliczenia związane z szyfrowaniem/deszyfrowaniem)
- koszty rozwiązania - większa złożoność powoduje zwiększenie kosztów zarówno samego sprzętu, jak i konfiguracji oraz późniejszej opieki nad tak wykonanym systemem

Najlepszym sposobem sprawdzenia podatności dowolnego systemu komputerowego są odpowiednie narzędzia - zarówno oprogramowanie, jak i narzędzia fizyczne. Oba rozwiązania mają swoje wady i zalety, jednak w znakomitej większości oprogramowanie konfiguracyjne udostępniane jest na licencji GNU, MIT czy LGPL. To pozwala używać go niemal każdemu bez ponoszenia dodatkowych kosztów.

Istnieje wiele projektów dostarczających gotowe rozwiązania do testowania i ujawniania słabości zarówno fizycznych (przykładowo niska przepustowość sieci, układy scalone z ujawnionymi fizycznymi lukami czy układy z błędami projektowymi, takimi jak złe dopasowanie mikroprocesora z układami pamięci) jak i logicznych (przykładowo słabe zabezpieczenie hasłowe, zastosowanie podatnego na atak protokołu komunikacyjnego czy wdrożenie słabego protokołu szyfrującego).
Każde ze wspomnianych rozwiązań cechuje się łatwością użytkowania, ilością dostarczonych gotowych do użycia narzędzi, sposobem zapisywania raportów z testowania systemów komputerowych czy też ilością obsługiwanych platform sprzętowych.

4. Przebieg.

Podczas laboratorium należy:

- zakładając wybór gotowego rozwiązania do testowania bezpieczeństwa systemów komputerowych, należy porównać dostępne na rynku oferty poszczególnych systemów testujących zabezpieczenia i skazać, według własnego uznania, najlepszy z nich. Wymagane będzie opisanie (co najmniej na 3 zdania) umotywowanie wyboru (przykładem gotowego rozwiązania jest chociażby BlackArch, aczkolwiek mile widziane będzie wybranie mniej popularnych rozwiązań, w tym płatnych)
- wskazać które narzędzia udostępnione w ramach wybranego systemu będzie najprzydatniejsza do testowania dowolnego, wybranego systemu informatycznego. Należy opisać co najmniej trzy narzędzia wraz z ich zastosowaniem (co dokładnie zostanie przez nie przetestowane). Mile widziane byłoby wskazanie działania i/lub wyników każdego narzędzia (o ile będzie to możliwe)
- należy wskazać, które z rozwiązań - oprogramowanie, gotowy system czy narzędzie sprzętowe - wedle własnego odczucia, będzie lepsze/skuteczniejsze do testowania dowolnego systemu komputerowego. Swój wybór należy rozsądnie uzasadnić. Kryteria doboru oraz wyboru należy do piszącego sprawozdanie

5. Zakończenie

Rozwiązanie należy przesłać w postaci PDF (NIE MUSI MIEĆ FORMY SPRAWOZDANIA!) na adres piotr_dobosz@int.pl, w temacie wiadomości zawierając frazę [AHNS_BSK].

6. Dodatki

https://brightsec.com/blog/security-testing/
https://thesecmaster.com/top-15-powerful-hardware-pen-testing-tools-for-successful-pen-testing/
https://github.com/mandiant/commando-vm
https://www.javatpoint.com/best-kali-linux-alternatives