UNSHADE

Katalog i zakres usług

Wersja 1.2
25.10.2022

1. Audyt aplikacji webowej

Audyt aplikacji webowej identyfikuje luki w zabezpieczeniach aplikacji webowych. Audyt wykonywany z poziomu dostępu do globalnej sieci Internet, obejmujący:

- Identyfikację serwisu, poszukiwanie domen zależnych, historycznych, poddomen. Krótka analiza dostępnej historii serwisu. Przeszukiwanie przestrzeni publicznej w poszukiwaniu wycieków danych.
- Identyfikację dostępnych środowisk testowych i deweloperskich.
- Identyfikację rodzaju oprogramowania działającego na serwerze oraz wykorzystywanych technologii.
- Manualne i automatyczne testy bezpieczeństwa znalezionych usług. Poszukiwanie podatnych wersji oprogramowania, błędów i luk w zabezpieczeniach czy domyślnych dostępów do systemów.

2. Audyt Active Directory

Audyt AD identyfikuje luki w zabezpieczeniach, symulując zagrożenie od strony wewnętrznego pracownika lub skompromitowanego hosta znajdującego się wewnątrz firmowej sieci. Obejmuje między innymi, takie działania jak:

- Identyfikację usług i serwerów działających w Active Directory.
- Manualne i automatyczne testy bezpieczeństwa znalezionych usług. Poszukiwanie podatnych wersji oprogramowania, błędów i luk w zabezpieczeniach czy domyślnych dostępów do systemów.
- Poszukiwanie nieprawidłowych konfiguracji usług i serwerów w Active Directory
- Działania z zakresu eskalacji uprawnień lokalnych i w domenie.
- Próby ekstrakcji wrażliwych danych bądź dostęp do krytycznych systemów.
- Sporządzenie raportu zawierającego znalezione błędy wraz ze szczegółowym opisem i instrukcje dotyczące załatania znalezionych luk. Konsultacja z ekspertem.
- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa.

3. Audyt LAN

Audyt wykonywany z poziomu dostępu do lokalnej sieci LAN, obejmujący między innymi:

- Identyfikację potencjalnie niebezpiecznych miejsc w LAN, które mogłyby posłużyć do ataków.
- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa.
- Sporządzenie raportu zawierającego znalezione błędy wraz ze szczegółowym opisem i instrukcje dotyczące załatania znalezionych luk. Konsultacja z ekspertem.

Podczas testu zostają wykonywane takie czynności jak:

- Mapowanie sieci.
- Identyfikacja urządzeń w sieci.
- Identyfikacja podsieci.
- Określenie usług dostępnych w LAN.
- Manualne i automatyczne testy bezpieczeństwa znalezionych usług. Poszukiwanie podatnych wersji oprogramowania, błędów i luk w zabezpieczeniach czy domyślnych dostępów do systemów.
- Weryfikacja ochrony i potencjalnych punktów dostępowych do sieci. Weryfikacja istniejących zabezpieczeń.

4. Audyt DMZ

Audyt wykonywany z poziomu dostępu do globalnej sieci Internet, obejmujący:

- Identyfikację potencjalnie niebezpiecznych miejsc, które mogą zostać zaatakowane bezpośrednio z Internetu.
- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa.
- Sporządzenie raportu zawierającego znalezione błędy wraz ze szczegółowym opisem i instrukcje dotyczące załatania znalezionych luk. Konsultacja z ekspertem.

Podczas testu zostają wykonywane takie czynności jak:

- Skanowanie portów, identyfikacja dostępnych usług, wersji systemów, używanego oprogramowania i urządzeń.
- Weryfikacja ochrony i potencjalnych punktów dostępowych do sieci. Weryfikacja istniejących zabezpieczeń, w tym WAF, Firewall i innych.
- Manualne i automatyczne testy bezpieczeństwa znalezionych usług. Poszukiwanie podatnych wersji oprogramowania, błędów i luk w zabezpieczeniach czy domyślnych dostępów do systemów.
- Opcjonalnie: wykonanie ataków typu Denial of Service (DoS).

5. Audyt WiFi

Audyt wykonywany w zasięgu wskazanej sieci bezprzewodowej lub w określonej lokalizacji. Operacje z zakresu tzw. WarDrivingu.

Obejmuje:

- Identyfikację potencjalnie niebezpiecznych miejsc, które mogą zostać zaatakowane z zewnątrz sieci.
- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa.
- Sporządzenie raportu zawierającego znalezione błędy wraz ze szczegółowym opisem i instrukcje dotyczące załatania znalezionych luk. Konsultacja z ekspertem.

Podczas testu zostają wykonywane takie czynności jak:

- Identyfikacja dostępnych sieci. Identyfikacja urządzeń sieciowych.
- Weryfikacja istniejących zabezpieczeń sieci. Weryfikacja ustawień bezpieczeństwa.
- Ataki mający na celu złamanie hasła dostępowego do sieci.
- Ataki na inne mechanizmy weryfikacyjne sieci (np. PIN WPS).

6. Audyt serwerów

Audyt wykonywany na wskazanym serwerze klienta. Obejmuje różne operacje, w zależności od charakterystyki rozwiązania. Przykładowe realizacje obejmują między innymi:

- Audyt serwera HTTP
- Audyt serwera S/FTP
- Audyt serwera pocztowego
- Audyt serwera bazy danych
- Audyt serwera VPN
- Audyt serwera monitoringu

Podczas audytu serwera w następuje weryfikacja obecnych mechanizmów bezpieczeństwa, wersji zainstalowanego oprogramowania, obsługi błędów, gromadzenia logów, weryfikacja architektury rozwiązania czy weryfikacja uprawnień. Dokładny zakres i przebieg testów zawsze ustalane są z klientem przed rozpoczęciem prac i dopasowane są one do konkretnego testowanego obiektu.

7. Audyt konfiguracyjny

Audyt wykonywany w zakresie wskazanego systemu/systemów IT. Obejmuje min.:

- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa. Hardening systemu.
- Weryfikację działania systemu AV.
- Weryfikację określonych uprawnień w systemie.
- Weryfikację usług udostępnionych.
- Weryfikację działających procesów i procesów cyklicznych/zaplanowanych.
- Weryfikację tworzenia i przywracania kopii zapasowych.
- Weryfikację aktualizacji systemu.
- Weryfikację systemów typu firewall.

8. Konsultacje

Konsultacja z ekspertem wybranych zagadnień związanych z bezpieczeństwem IT. Przykładowymi tematami konsultacji są:

- Wdrożenie nowego rozwiązania.
- Ocena obecnych zabezpieczeń.
- Analiza kodu źródłowego aplikacji.
- Analiza systemów monitoringu, detekcji, zbierania logów.
- Bezpieczeństwo w procesie tworzenia oprogramowania (SSDLC).
- Analiza rozwiązań kryptograficznych.
- Opinie nt. bezpieczeństwa sieci i aplikacji.
- Standardy i dokumentacje.
- Doradztwo produktowe.

Eksperci dobierani są pod kątem określonych tematów konsultacji, a w ramach jednej konsultacji może uczestniczyć ich wielu. Konsultacje przeprowadzane są przez specjalistów z minimum 5 letnim doświadczeniem w branży oraz certyfikatami potwierdzającymi ich umiejętności. Wśród posiadanych przez naszych konsultantów certyfikatów są między innymi: CEH, OSCP, OSEP, CRTP, CRTE, CCENT, CCNA, PACES, CARTP, eCPPTv2, eCPTX, CRTO.

9. Odzyskiwanie haseł

Odzyskujemy offline hasła do plików, usług i systemów. Warunkiem jest dostarczenie pliku, urządzenia, skrótu (hash), bądź innej informacji na podstawie której możliwe będzie przeprowadzenie procesu odzyskiwania.

Odzyskujemy hasła do różnych formatów plików, między innymi:

- pdf
- zip
- programy office
- keepass
- Płatnik

Oraz określonych algorytmów, np.:

- bcrypt
- MD
- SHA

i wielu innych. Odzyskujemy hasła do zaszyfrowanych dysków i pendrive.

Odzyskiwanie wykonywane jest za pomocą wielu sposobów, np. słowników, brute-force i mieszanych. Odzyskiwanie przeprowadzone jest zarówno autorskimi metodami i narzędziami oraz narzędziami publicznie znanymi (min. hashcat i jtr). Usługa wykonywana jest z użyciem lokalnego sprzętu autorskiej konstrukcji, opartego na kartach graficznych nvidia GTX i RTX.

10. OSINT i pozyskiwanie informacji

Celem operacji typu OSINT jest zebranie jak najwięcej informacji. Ten audyt symuluje pierwszy etap bardziej rozbudowanego ataku na firmę/organizację i odpowiada na popularne pytanie “Czego można się o nas dowiedzieć z Internetu?”. Obejmuje między innymi:

- Zestaw informacji o potencjalnych metodach przeprowadzenia ataku na podstawie publicznych źródeł.
- Poszukiwanie informacji o infrastrukturze firmy dostępnej z Internetu. Informacje o serwerach, domenach, stronach internetowych.
- Poszukiwanie informacji o pracownikach - stanowiskach, adresach e-mail, numerach telefonów.
- Poszukiwanie informacji historycznych oraz w archiwach.
- Raport zawierający potencjalnie istotne dane, które można znaleźć o firmie/osobie z publicznie dostępnych źródeł.

11. Wejście fizyczne

Audyt wykonywany na miejscu, w siedzibie klienta. Obejmuje:

- Identyfikację potencjalnie niebezpiecznych miejsc, które mogą zostać zaatakowane z zewnątrz/wewnątrz biura.
- Ocenę aktualnie stosowanych zabezpieczeń i sugestie dotyczące rozbudowy i ulepszeń systemów bezpieczeństwa.
- Sporządzenie raportu zawierającego znalezione błędy wraz ze szczegółowym opisem i instrukcje dotyczące zmian. Konsultacja z ekspertem.

Podczas testu zostają wykonywane takie czynności jak:

- Identyfikacja luk w procedurach oraz edukacji i świadomości pracowników.
- Fizyczne wejście do biura firmy i wykonanie celu zadania - np. pozostawienie wiadomości, ekstrakcja danych.

12. Testy socjotechniczne

Audyt obejmujący testy socjotechniczne symulujące prawdziwy atak na organizację. Podczas testów wybierana jest konkretna osoba lub grupa, od której następuje próba pozyskania kluczowych informacji. Testy socjotechniczne służą wyłudzeniu takich informacji, jak np:

- Dane dostępowe do systemów firmowych takich jak poczta, czat, VPN, systemy obsługi klienta, systemy administrujące, systemy bezpieczeństwa fizycznego i inne.
- Dane kontaktowe, w tym adresy email i numery telefonu.
- Dane dotyczące infrastruktury organizacji.
- Dane dotyczące rozwiązań bezpieczeństwa stosowanych w organizacji.
- Dane dotyczące lokalizacji stanowisk, przedmiotów i osób.

i wiele innych, charakterystycznych dla danej firmy/organizacji.

Testy mogą być przeprowadzane również wyłudzenia konkretnych informacji. Takie audyty opierają się na testach typu “czy osoba A otworzy załącznik”, “czy osoba B wejdzie w link”, lub “czy osoba C włoży pendrive do swojej stacji roboczej”.

Po przeprowadzeniu testów socjotechnicznych, przeprowadzamy również szkolenia dla pracowników. Edukujemy i uświadamiamy personel, że bezpieczeństwo zaczyna się od ludzi.

13. Szkolenia

Oferujemy szeroką gamę szkoleń dopasowanych bezpośrednio do potrzeb zamawiającego. Nasi specjaliści przygotowywali szkolenia między innymi z:

- Cybersecurity awareness - szkolenie dla pracowników nietechnicznych.
- Podstawy rozproszonego łamania haseł.
- Bezpieczeństwo aplikacji webowych.
- Bezpieczeństwo systemu linux.
- Jak pisać bezpieczny kod? Szkolenie dla programistów PHP.
- Jak wdrożyć rozwiązania security w CI/CD?