Penetrační testování mobilních platforem

Penetrační testy, které jsou zaměřeny na vyhledávaní bezpečnostních chyb a zranitelností mobilních aplikací. Testy v této kategorii jsou rozděleny do třech logických celků. Jsou prováděny jak standardizované testy, tak vyšetřovací techniky představující jedinečné know-how, které je získáváno na základě kontinuálního bezpečnostního výzkumu členů Penetrační laboratoře FAI.

Testy zaměřené na datovou bezpečnost:

- **String Digging;**
- **Content Provider Leakage;**
- **Insecure File Storage;**
- **SQLite3 zranitelnosti;**
- **Získávání citlivých dat pomocí Reverse Engineeringu;**
- **Log Leakage.**

Testy zaměřené na síťovou komunikaci:

- **Zachytávání a následná analýza síťového provozu;**
- **Testy zaměřené na odolnost vůči modifikaci síťového provozu;**
- **Zjišťování odolnosti proti MiTM.**

Testy zaměřené na aplikační zranitelnosti:

- **Identifikace Attack Surface vyšetřovaných aplikací;**
- **Bezpečnostní analýza souboru AndroidManifest.xml;**
- **Attacking Authentication;**
- **Authentication Bypass;**
- **Testovaní odolnosti uživatelských vstupů (Input Validation);**
- **Broken Cryptography.**

Sestavení konkrétních testů do většího testovacího celku je pak prováděno přímo na základě individuálních potřeb zákazníka. Výstupem testovacího procesu je standardizovaná závěrečná zpráva (Mobile Pentest Report), která obsahuje nejen popis všech nalezených bezpečnostních rizik, ale i doporučené postupy k jejich odstranění.

Poradenská činnost

Mezi aktivity laboratoře patří nejen penetrační testování, ale zabývá se také konzultační činností v oboru bezpečnosti informační infrastruktury. Nabízí poradenské služby a pomoc při řešení otázek zabezpečení IT infrastruktury.

Laboratoř nabízí konzultační služby v oblastech:

- **Zabezpečení operačních systémů:** návrh a implementace serverů.
- **Zabezpečení mobilních platforem:** zabezpečení mobilních zařízení na platformě Android.
- **Analýza malwaru pro mobilní platformy:** analýza chování a zaměření malwaru na mobilní platformě Android.
- **Návrh a implementace počítačových sítí:** návrh, implementace a zabezpečení síťové infrastruktury. Metodika používání a ochrany bezdrátových sítí.
- **Návrh a implementace webových portálů:** návrhy zabezpečení portálu. Kontrola implementace a použití bezpečnostních zásad.
- **Řešení problematiky BYOD:** specifikace omezení BYOD. Návrh a implementace zabezpečení infrastruktury při použití modelu BYOD.
- **Prevence útoků:** návrh a implementace monitoringu v oblasti počítačových sítí a serverů.
- **Návrh bezpečnostních politik:** tvorba bezpečnostních politik. Kontrola platnosti politik. Aktualizace politik dle aktuálních ohrožení.
- **Školení správců IT:** bezpečnostní školení pro správce IT infrastruktur.
- **Školení zaměstnanců:** bezpečnostní školení pro zaměstnance firem.
- **Řešení bezpečnostních incidentů v IT:** pomoc se zpracováním bezpečnostního incidentu. Návrh vhodných protiopatření.
- **Řešení bezpečného vzdáleného přístupu:** návrh a implementace zabezpečeného vzdáleného připojení do firemní infrastruktury.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

CEBIA-Tech
Centrum bezpečnostních, informačních a pokročilých technologií

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Nad Stráněmi 4511
760 05 Zlín
Česká republika
GPS: 49°13'50.991"N, 17°39'26.257"E

Ředitel Centra
prof. Ing. Vladimír Vašek, CSc.
Telefon: +420 576 035 255
E-mail: vasek@fai.utb.cz
vopatrilova@fai.utb.cz

Kontakt
Ing. David Malaník, Ph.D.
Telefon: +420 576 035 065
E-mail: dmalanik@fai.utb.cz

Těšíme se na spolupráci!

www.cebia.utb.cz

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

CEBIA-Tech
Centrum bezpečnostních, informačních a pokročilých technologií

VTP ICT
Vědecko-technický park
Informační a komunikační technologie

VÝZKUMNÝ PROGRAM 1
„APLIKACE INŽENÝRSKÉ INFORMATIKY“
Vědecko-výzkumná a vývojová činnost:
PENETRAČNÍ TESTOVÁNÍ

PT LAB
Penetration Testing Laboratory
http://ptlab.fai.utb.cz

Univerzita Tomáše Bati ve Zlíně

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

Penetrační testování

Novou součástí Regionálního výzkumného centra bezpečnostních, informačních a pokročilých technologií (RVC CEBIA-Tech), se na začátku roku 2016 stala Laboratoř pro penetrační testování (PTLAB.fai.utb.cz).

Penetrační testování simuluje reálné útoky, kterým může být vystavena libovolná část infrastruktury kterékoliv firmy, a to i bez ohledu na to, zda je nebo není připojena k síti Internet.

Tester v tomto případě vystupuje v pozici reálného útočníka (hackera) a snaží se o překonání bezpečnostních mechanismů svého cíle. Jediným rozdílem proti reálnému útoku je minimalizace možných škod způsobených testováním: nedochází tak např. k cílenému zavirování testované infrastruktury. Jednotlivé testy jsou tedy primárně nedestruktivního charakteru.

Součástí všech typů penetračních testů je také soubor doporučení pro odstranění nalezených zranitelností.

Laboratoř je schopna realizovat následující operace:

- **Penetrační testování operačních systémů:** testy zabezpečení serverů i klientských PC s operačními systémy Microsoft Windows, Linux, MAC OSX.
- **Penetrační testování síťové infrastruktury:** testy zaměřené na softwarové i hardwarové zabezpečení drátových i bezdrátových sítí.
- **Penetrační testování webových portálů:** testy jednoduchých webových stránek, e-shopových portálů, redakčních systémů i intranetových stránek.
- **Penetrační testování mobilních platforem:** testy zaměřené na hodnocení zabezpečení mobilních aplikací (Mobile Application Security Assessment).

Nabízí poradenskou činnost při:

- Návrhu zabezpečení serverů i klientských PC;
- Návrhu bezpečných síťových infrastruktur;
- Návrhu a implementaci bezpečnostních politik;
- Implementaci webových portálů a intranetových řešení;
- Vývoji bezpečných mobilních aplikací;
- Řešení problému se systémem BYOD;
- Řešení IT bezpečnostních incidentů.

Penetrační testy operačních systémů

V této části se jedná o realizaci testů (hackerských útoků), které se zaměřují na konkrétní fyzické servery a jednotlivé klientské počítače.

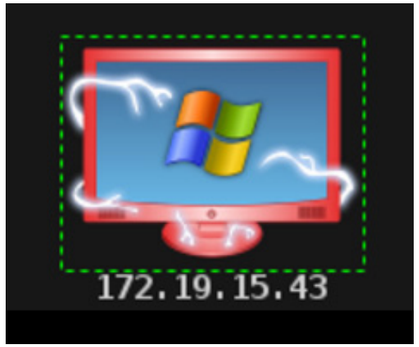
Testy jsou zaměřeny na běžící operační systémy (Microsoft Windows, Linux, MAC OSX) a na možné zranitelnosti v nich. Další testovanou skupinou jsou běžící služby a i samotná politika hesel dané organizace.

Oblasti testování:

- **Detekce otevřených portů:** hledání nezabezpečených portů na daném serveru/PC.
- **Detekce běžících služeb:** identifikace běžících síťových aplikací a jejich konkrétních verzí.
- **Exploitace jednotlivých OS:** testy na úrovni zabezpečení operačního systému jako takového. Jedná se o hledání zranitelností přímo v operačním systému.
- **Exploitace běžících služeb:** testy služeb/aplikací, které na serveru běží.
- **Hledání zranitelných uživatelských účtů:** hledání defaultních uživatelských účtů, účtů bez hesla nebo účtů s triviálními hesly.
- **Útoky na hesla uživatelů:** slovníkové útoky na hesla uživatelů.
- **Detekce Lock-out politik:** hledání politik uzamčení účtu.
- **Testy reakcí na útoky DOS/DDOS:** testy odolnosti proti DOS a DDOS útokům.

Typy testů:

- **Průzkum cíle:** získání všech dostupných informací o testovaném objektu.
- **Útok s vědomím administrátorů:** útok na nalezené zranitelnosti s předchozím informováním IT správců.
- **Skrytý útok ze známého zdroje:** útok bez předchozího upozornění správců IT, vedený z našeho adresného rozsahu.
- **Skrytý útok z neznámého zdroje:** útok bez předchozího upozornění správců IT, vedený z anonymního adresného rozsahu.
- **Útok z vnitřní sítě společnosti:** simulace útoku, např. nespokojeného zaměstnance.



Penetrační testy síťové infrastruktury

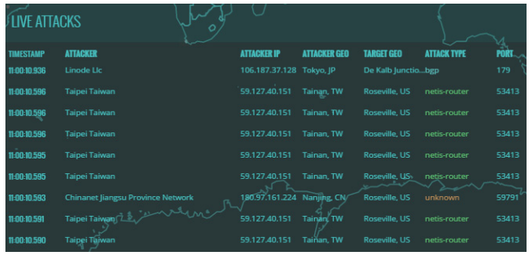
Tyto testy jsou zaměřeny na bezpečnost počítačových sítí, které jsou v dané společnosti zastoupeny. Testy se zaměřují jak na klasické kabelové sítě, tak i na bezpečnost bezdrátových sítí. Spadají zde i testy oddělení jednotlivých sítí: např. oddělení sítě pro hosty od zbytku infrastruktury.

Oblasti testování:

- **Bezpečnost implementace sítí:** hledání zranitelných míst síťové infrastruktury.
- **Používané komunikační protokoly:** analýza používaných komunikačních protokolů s ohledem na jejich bezpečnost.
- **Běžící síťové služby:** identifikace všech běžících služeb/aplikací v síti.
- **Možnosti odposlechu komunikace:** detekce použití komunikačních protokolů, které nemají ochranu přenášeného obsahu.
- **Omezení sítě pro hosty:** dostupnost firemního segmentu pro uživatele síťového segmentu určeného pro návštěvy.

Typy testů:

- **Inventarizace přístupových bodů drátové sítě:** hledání možných bodů vniku do síťové infrastruktury; hledání slabě zabezpečených prvků sítě.
- **Omezení přístupů z drátových sítí:** detekce metod omezení přístupu k síti; detekce metod přidělování IP adres a autentizace přístupu.
- **Průzkum bezdrátových sítí:** hledání všech dostupných bezdrátových sítí v daném objektu; detekce omezení přístupu k sítím a systému přidělování IP adres.
- **Získání neoprávněného přístupu k síti:** prolomení zabezpečení sítě.
- **Podvržení Access Pointu:** možnost podvržení AP organizace a odposlech na podvržené síti.
- **Odposlech komunikace:** odposlech komunikace probíhající na síti, detekce hesel a obsahu komunikace.
- **Útoky MiTM:** sofistikované útoky na specifické cíle dané infrastruktury.
- **Útoky na aktivní prvky sítí:** lámání hesel k jednotlivým aktivním prvkům infrastruktury.



Penetrační testování webových portálů

Testy uvedené v této kategorii se zaměřují na bezpečnost webových stránek a portálů postavených na webových technologiích. Je možné testovat jak webové portály, které jsou umístěny v síti Internet, a jsou tedy dostupné komukoliv, tak i intranetové řešení. Zvláště v oblasti intranetových řešení, je bezpečnost obvykle podceňována, protože z pohledu správců je přístup k Intranetu omezen „pouze“ na zaměstnance dané společnosti.

Oblasti testování:

- **Bezpečnost obsahu:** odolnost obsahu před neautorizovanou změnou útočníkem.
- **Metody autentizace backendu:** zabezpečení backendu aplikace před neoprávněným přístupem.
- **Chyby v řízení přístupu:** neošetřené přímé přístupy ke chráněným datům webového portálu.
- **Použití zranitelných komponent:** detekce použití komponent se známou zranitelností.
- **Neošetřená pole formulářů:** možnosti manipulace s webem pomocí uživatelských vstupů.
- **Zabezpečení databází:** možnosti přístupu do databáze webového portálu.

Typy testů:

- **Injektování kódu:** neautorizované vložení dat do databáze portálu - SQL injection.
- **Překonání autentizace:** slovníkové útoky na hesla, prolomení autentizace do backendu aplikace.
- **Neoprávněná úprava obsahu:** změna vzhledu portálu, úprava kódu portálu.
- **Expozice citlivých dat:** přístup k privátním datům webového portálu.
- **Nezabezpečené odkazy na objekty:** testování zranitelnosti předávaných parametrů webových stránek, přímý přístup k datům pomocí úprav předávaných parametrům.