Postrehy z penetračných testov

Ing. Zuzana Vargová
CSIRT.SK

SASIB 22.3.2017

CSIRT.SK
www.csirt.gov.sk

CSIRT a penetračné testovanie

- Od roku 2013
- Penetračné testovanie inštitúcií VS
  - Interné penetračné testy
  - Externé penetračné testy
- Prevencia – proaktívna služba

Čo je penetračný test

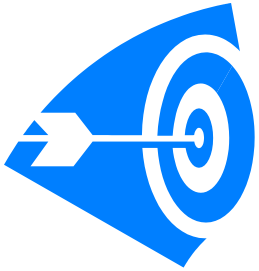
- Skrátene *pentest*, je

autorizovaný
simulovaný
útok na informačný systém, ktorý
odhaľuje bezpečnostné nedostatky, a pri ktorom potenciálne *získame prístup k systému* a/alebo *dátam*.

Typy testov

- Pozícia a predmet:
  - Interné
  - Externé

- Dostupné informácie
  - Black box
  - Grey box
  - White box



- Spôsob testovania
  - Automatizované
  - Manuálne

Mýty a legendy o internej sieti...

- „Naša interná sieť je dôveryhodná... Veď máme firewall (IDS/IPS/Strážneho Jednorožca), útočníci sa sem zvonka nedostanú a vnútorná sieť je celkom bezpečná.“
- „Naši používatelia by také niečo nedokázali.“
- „Váš pentest nie je dobrý. Už sme boli testovaní, a NIČ sa nenašlo!“

… a externých systémoch

- „Predstavuje reflexné XSS skutočne problém? O čo vlastne ide?“
- „No a čo, že sa zobrazuje chyba databázy? Aspoň používateľ vie, že zadal chybný vstup…“
- „Ten systém, ktorého databázy ste cez to SQL Injection stiahli, je starý. Dáta nemajä až takú hodnotu…“

Rúcanie mýtov

- Nie, nie, nie, žiadna sieť nie je absolútne dôveryhodná. Možno tak váš PC odpojený zo siete. Zaliaty betónom v olovenej skrinke. Na dne oceána.
  - Malware v pošte
  - USB
  - Sociálne inžinierstvo - Shoulder-surfing, falošný admin *(Prosím, zmeňte si heslo na...)* a podobne

- Nezáleží na tom, čo používateľ dokáže, ale čo dokáže malware, ktorý sa na jeho PC môže dostať.
- Množstvo hackerských nástrojov je extrémne jednoduchých a používateľsky prítulných – zvládne s nimi pracovať aj script kiddie.

- Akceptovať len pozitívne správy a poprieť zistené fakty nie je celkom zdravý prístup...

Rúcanie mýtov

- Nuž, ak nezáleží na bezpečnosti používateľov, tak ani XSS nemusí byť problém. Ale aj administrátor je používateľ...
- Iste, slobodný prístup k informáciám je fajn vec. Ak to chceme rozšíriť aj na zverejnenie podrobností, kde v databáze aký vstup nekontrolujeme, rátajme, že slobodne prístupné môžu byť onedlho všetky dáta z databázy.
- Prečo je starý zraniteľný systém teda vôbec tu?

Slabé ohnivko I: zastarané systémy

- Exploitácia zastaranej verzie OS – Windows Server 2003... Alebo XP!
  - (XP nie je podporovaný od apríla 2014, Server 2003 od júla 2015)
- Exploitácia zraniteľnej verzie zálohovacieho systému
- Exploity Metasploit Frameworku, bez úpravy či obfuskácie!
  - Aj začiatočník to zvládne...

Slabé ohnivko II: zjednodušenie administrácie

- zápis doménových politík do súboru dostupného doménovým používateľom
  - *.xml* súbor, obsahujúci účet lokálneho administrátora pracovných staníc spolu s heslom, hashovaným v reverzibilnom formáte
  - Prístup ku všetkým spravovaným staniciam
  - Má administrátor DEBUG privilégium?

Slabé ohnivko III: Keď každý ladí, niečo neladí...

- DEBUG privilégium
  - Umožňuje používateľovi pripojiť k procesu alebo jadru OS debugger
  - Vývojár programu potrebuje mať toto privilégium, pretože mu umožňuje ladiť program.
  - V produkčnom prostredí by DEBUG malo byť v maximálnej možnej miere obmedzené.
    - V reálnom svete ho mávajú aj bežní používatelia...
- Proces lsass.exe – v pamäti sa ukladajú údaje z prihlásení Vzdialenej pracovnej plochy (RDP)...
  - Útočník ako bežný používateľ získa dump pamäte a jej analýzou získa credentials v otvorenom tvare.
  - K dispozícii je na tento účel viacero voľne dostupných nástrojov, umožňujúcich lokálne aj vzdialené získanie autentifikačných dát.
- ! Preto monitorovať Windows Security log...
- ! Restricted admin account

Slabé ohnivko IV: Ťažko veci meníme...

- Spätná kompatibilita
  - Integrácia so starými systémami => vypnutie ochrán nových OS
  - Príklad – Windows:
    - Od Windows Vista je vypnuté ukladanie LM hashov
      - Občas je zapnuté...
    - Ukladanie doménových hesiel použitím reverzibilného šifrovania od Servera 2003 takisto...
      - ... a tiež je občas zapnuté.
    - Autentifikácia pomocou protokolu Kerberos nie je realisticky rozbiteľná
      - Treba ju však nastaviť na kompatibilných zariadeniach, a pristupovať k nim cez doménové meno...

Slabé ohnivko V: Sme len ľudia...

- Heslá
  - Heslo123, <menoFirmy>951, mamina1, Marec2017!, <menoPsik@>, <rodneMesto>789, <menoPos1edn3jPriat3ľky>, ... NIE SÚ HESLÁ!!!
  - Prečo sa heslá menia každé 3 mesiace? Riziká:
    - používateľ si nové heslo nepamätá, tak si ho zapíše
    - Zvolí heslo podľa politík: 8+ znakov, veľké/malé, písmeno/číslo, špeciálny znak.

Slabé ohnivko V: Sme len ľudia...

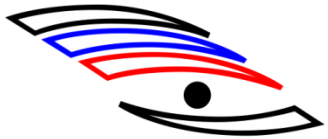
- Heslá
  - Heslo123, <menoFirmy>951, mamina1, Marec2017!, <menoPsik@>, <rodneMesto>789, <menoPos1edn3jPriat3ľky>, ... NIE SÚ HESLÁ!!!
  - Prečo sa heslá menia každé 3 mesiace? Riziká:
    - používateľ si nové heslo nepamätá, tak si ho zapíše
    - Zvolí heslo podľa politík: 8+ znakov, veľké/malé, písmeno/číslo, špeciálny znak.

Marec2017+

Slabé ohnivko VI: Pozrieme sa všade, ak nám dovolia.

- Aj malware na našom PC.
  - Problém so segmentáciou siete
  - Diferenciácia rolí
    - Prečo má používateľ DEBUG privilege?
    - Prečo sa administrátor servera môže prihlásiť na konzolu centrálneho switcha?
    - Prečo sa POUŽÍVATEĽ môže prihlásiť na konzolu centrálneho switcha?
  - A tak ďalej...

Otázky



CSIRT.SK
www.csirt.gov.sk

Ďakujem za pozornosť!

zuzana.vargova@csirt.sk

CSIRT.SK
www.csirt.gov.sk