PENETRAČNÉ TESTY

Prevencia pred únikom dát

Agenda

- O mne
- Čo sú penetračné testy a prečo ich vykonávať ?
- Čo sa dá testovať ?
- Typy testov
- Priebeh testovania
- Ako si vybrať ?
- Metodiky
- Výstupy testovania
- Riziká spojené s testovaním
- Chyby pri zadaní testu

O MNE...

O mne

Tomáš Ležovič

Penetračný tester v spoločnosti ESET spol s.r.o.

V minulosti:

- Sieťový / Server admin
- Web app / Mobile app developer

ČO SÚ PENETRAČNÉ TESTY A PREČO ICH VYKONÁVAŤ ?

Čo sú penetračné testy a prečo ich vykonávať ?

Čo:

- Simulácia skutočného útoku

Prečo:

- Rýchly rozvoj sieťových technológií
- Časté incidenty
- Medializácia

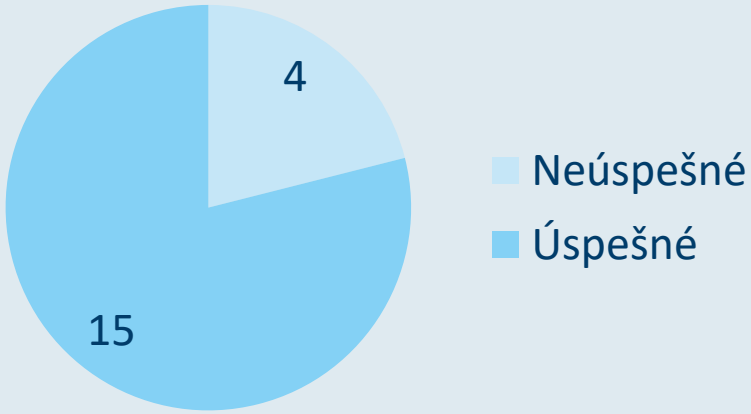
ČO SA DÁ TESTOVAŤ?

Čo môžeme testovať na bezpečnosť ?

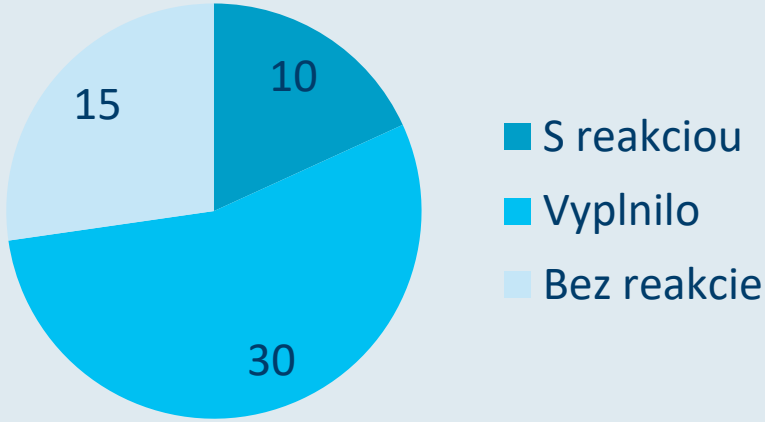
- Sieťová infraštruktúra
  - bezdrôtové technológie
- Aplikačná infraštruktúra
- Aplikácie
- Klientske zariadenia
- Verejné terminály
- Priemyselné zariadenia
- Procesy
- Ľudia
- Fyzické zabezpečenie

Štatistika Soc. inžinierstva

Volania



Email



TYPY TESTOV

Čo môžeme testovať na bezpečnosť ?

Test známych zraniteľnosti

(Vulnerability Assessment)

- Široký záber
- Automatizovaný
- Množstvo false positive

Bezpečnostný audit

(Security Assessment)

- Stojí medzi VA a Pentestom
- Veľká škála možností

Penetrační test

(Penetration Test)

- Pevne daný ciel
- Postup do hĺbky
- Simulácia skutočného útoku
- Preverujú sa aj procesy

Testy známych zraniteľností

- Zmapovanie maximálneho množstva zraniteľností
- Ide do šírky
- Z pravidla obmedzené iba na využití automatizovaných nástrojov
- Nízka miera podielu ľudskej práce
- Nájdené zraniteľnosti nie sú overované
- Vyššia miera „false negative“ a „false positive“ nálezov.
- Potenciálne nízky negatívni dopad v priebehu testovania

Bezpečnostný audit

- Zmapovanie maximálneho množstva zraniteľností, ide do šírky
- Súčasťou je skenovanie zraniteľnosti automatizovanými nástrojmi
- Nie je zameraný na test známych zraniteľností
- Stredná miera ľudskej práce
- Odhalené zraniteľnosti sa ručne overujú
- Ručné vyhľadávanie zraniteľností
- Nižšia miera „false negative“ a „false positive“ nálezov
- Možnosť regulovať negatívny dopad v priebehu testovania

Penetračný test

- Sleduje pevne stanovený ciel
- Nepokrýva všetky zraniteľnosti – sústredí sa na zneužiteľné
- Ide do hĺbky
- Vysoká miera ľudskej práce – manuálne vyhľadávanie zraniteľností
- Nájdene zraniteľnosti sú overované
- PoC formou exploitácie
- Nízka miera „false negative“ a „false positive“ nálezov
- Potenciálne vysoký negatívny dopad behom testovania

PRIEBEH TESTOVANIA

Priebeh testovania

- Príprava testu – definícia rozsahu, prístupov, cieľov
  - 1. Zber informácií– nepriamo, priamo
  - 2. Skúmanie (enumerácia, mapovanie)

- Konzultácia ďalšieho postupu so zadávateľom
  - 3. prienik do systému (exploitácia)
  - 4. Udržanie si prístupu – hacker

- Analýza, správa a prezentácia

Test vs skutočný útok

Z pohľadu vykonávaných činnosti prakticky totožné, až na :

- Techniky a používané nástroje sú rovnaké, alebo veľmi podobné
- Líšia sa v netechnických veciach
  - povolenie, dohodnutý rozsah a prístup, metodika
  - Informácie o testovaní, správa, priebeh
  - Časové obmedzenie
  - 1 vs mnoho
  - Nie je nutná dekompilácia, hrubá sila

AKO SI VYBRAŤ?

Čo zvážiť pred zadaním testu

- Predmet testov– aplikácia, infraštruktúra, procesy
- Čo je cieľom testu– najhoršie scenáre
- Z akej perspektívy, akého útočníka majú testy simulovať
  - interný vs. externý , znalosť prostredia
- Dopad na testované ciele, výber prostredí – testovacie vs. produkčné
- Doba realizácie, Metodika, Správa, …

METODIKA

Metodika

- Zaistí postup, úplnosť

- Webové - OWASP TG, OWASP TOP 10
- Mobilné - MSTG, MASVS
- Rôzne - OSSTMM, PTES

VÝSTUPY TESTOVANIA

Výstupy testovania

- Manažérske zhrnutie
- Popis testov
- Popis zistení / prienikov
- Odporúčané opatrenia
- Na vyžiadanie aj iné.. Screenshoty, videá..

Výsledky – hodnotenie závažností

- Zjednodušené - nízka - critical
- CVSS – bez vzdialeného prístupu nepoužiteľná
- OWASP DREAD
- OWASP RISK

RIZIKÁ SPOJENÉ S TESTOVANÍM

Riziká spojené s testovaním

NEINVAZÍVNY PENETRAČNÝ TEST

NEEXISTUJE

Riziká spojené s testovaním

- DoS
- Poškodenie dát
- Veľké množstvo nových záznamov

- Hostingové služby
- Testovanie DoS

NEDOSTATKY PRI ZADANÍ TESTU

Nedostatky pri zadaní testu

- Druh testu
- Garancia negatívneho dopadu
- Vopred požadované scenáre
- DoS a DDoS
- Nedostatočné podklady

Nedostatky pri zadaní testu

- Bez možnosti vidieť aplikáciu vopred
- Časové obmedzenia
- Chýbajúce dáta
- Zbytočné testy
- Chýbajúca súčinnosť – kontaktná osoba

SECURITY DAYS

ĎAKUJEM ZA POZORNOSŤ

Viac Info:

http://bit.ly/2DpdSeY

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE