Penetrační testování – co to je, jak na ně vč. odkazů a zdrojů

Popis

Penetrační test je provedení testu s cílem identifikovat zranitelnosti, které by mohly být přítomny v aktivu: na počítači, serveru, v informačním systému, síti, aplikaci nebo v organizaci (pak se testuje zranitelnost osob a fyzické zabezpečení). Penetrační testy provádí vyškolení, kvalifikovaní experti s použitím postupů, které předpokládají, že by mohli použít skuteční hackeři. Penetrační testy odhalují slabiny (zranitelnosti) i způsoby (hrozby), jakými by mohla být aktiva zneužita a poskytují návod, jak snížit existující riziko. Penetrační testy také mohou identifikovat schopnost organizace reagovat na incident bezpečnosti informací.

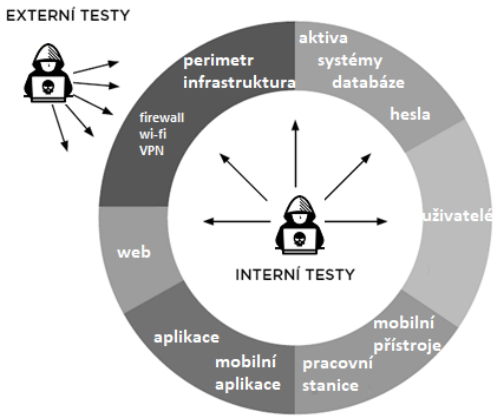
Účel penetračního testu

Identifikovat rizika a/nebo potvrdit rizikový scénář (scénáře).
Ujistit se o úrovni zabezpečení před předáním aktiva, aplikace nebo služby do provozu.
Ujistit na vyžádání zákazníka a/nebo partnera o zabezpečení aktiva, aplikace nebo služby .
Prokázat náležitou péči (due diligence) s ohledem na rizika bezpečnosti informací.
Zajistit shoda se zákonem, předpisy nebo smluvními požadavky (audit, compliance).

Typová rozdělení

Dle umístění pentestera

- Externí penetrační testy
  Externí penetrační test, např. infrastruktury, reprezentuje snahu anonymního útočníka o narušení firemní sítě z internetu s cílem obejití bezpečnostních kontrol, využití zranitelností a získání neoprávněného přístupu do sítě, případně s cílem znepřístupnění poskytované služby.
  Cíle externích testů: DMZ, e-mail, DNS, web server, webová aplikace ap.
- Interní penetrační testy
  Cílem interního penetračního testu, např. infrastruktury, je ověřit odolnost firemní sítě z vnitřní strany. Interní penetrační test bývá nejčastěji realizován z pohledu anonymního útočníka s fyzickým přístupem do vnitřní sítě bez přístupu k adresářovým službám anebo z pohledu zaměstnance s přístupem k adresářovým službám.
  Cíle interních testů: servery (fyzické i virtuální), operační systémy, jiné sw služby (webové servery, databáze, …).



Dle znalosti prostředí

- **black box pentesty**
  Penetrační tester je v roli průměrného hackera bez interních znalostí cílového systému. Testeři nejsou vybaveni žádnými znalostmi architektury nebo zdrojovým kódem, pokud není veřejně dostupný. Test se používá k určení chyb zabezpečení v systému, které lze zneužít mimo síť. Tester musí být obeznámen s automatizovanými skenovacími nástroji a metodikami pro ruční penetrační testování. Testeři musí být schopni vytvořit mapu cílové sítě na základě svých pozorování. Díky omezeným znalostem poskytnutým penetračnímu testeru jsou testy nejrychlejší, protože doba trvání do značné míry závisí na schopnosti testera lokalizovat a zneužít zranitelnosti v navenek publikovaných službách. Hlavní nevýhodou tohoto přístupu je, že pokud testeři nemohou prolomit perimetr, jakákoli zranitelná místa interních služeb zůstávají neobjevená a neopravená.

- **grey box pentesty**
  Je dalším krokem po black box testování. Pokud předchozí pentester zkoumá systém z pohledu cizince, teď tester má úroveň přístupu a znalostí uživatele, potenciálně se zvýšenými oprávněními v systému. Pentesteři mají obvykle určité znalosti o interních sítích, potenciálně včetně dokumentace k návrhu, architektuře a interních účtech sítě.
  Účelem průniku je poskytnout cílenější a efektivnější posouzení bezpečnosti sítě než posouzení black box. Pomocí projektové dokumentace pro síť mohou pentesteři zaměřit své úsilí v oblasti hodnocení na systémy s největším rizikem a hodnotou od začátku, spíše než trávit čas určováním těchto informací sami. Interní účet v systému také umožňuje testování bezpečnosti uvnitř perimetru a simuluje útočníka s dlouhodobějším přístupem k síti.

- **white box pentesty**
  Pentest white box má několik různých názvů, např. i clear-box, open-box, pomocné a logické testy. Spadá na opačný konec spektra od testování black box: penetrační testeři mají plný přístup ke zdrojovému kódu, dokumentaci architektury atd. Hlavní výzvou testování je nutnost prosévání obrovského množství dostupných dat k identifikaci potenciálních zranitelností, což z něj činí časově nejnáročnější typ penetračního testování.
  Na rozdíl od předchozích jsou pentesteři schopni provádět statickou analýzu kódu, přičemž používají analyzátory zdrojového kódu, ladicí zařízení a podobné nástroje, důležité pro tento typ testování. Nástroje a techniky dynamické analýzy jsou však také důležité, protože statická analýza může přehlédnout chyby zabezpečení, způsobené chybnou konfigurací cílových systémů.
  Pentestování white box poskytuje komplexní posouzení vnitřních i externích zranitelností, což z něj činí nejlepší volbu pro testování.

Výhody a nevýhody penetračních testovacích metodik

Pokud by všechny metodiky pentestingu fungovaly stejně dobře, použila by se pouze jedna z nich. Hlavními rozdíly mezi penetračními testováními black, gray a white box je přesnost testu a jeho rychlost, účinnost a pokrytí (záběr).

Účelem penetračního testování je identifikovat a opravit chyby zabezpečení, které by útočník zneužil. Proto ideální formou penetračního testování by proto byla metoda black box, protože většina útočníků nemá před zahájením útoku znalosti o vnitřním nastavení svého cíle. Průměrný útočník má však mnohem více času věnovat se útočnému procesu než průměrný pentester, takže ostatní metody penetračních testů byly vyvinuty tak, aby se snížila doba provádění zvýšením množství informací, poskytnutých testerovi.

Dalším extrémem u pentestování white box, kde pentesterům jsou poskytnuty úplné informace o cílovém systému. Problém s tímto typem pentestu je, že množství informací způsobí, že pentesteři budou jednat jinak než black box (tj. opravdoví) hackeři, což je potenciálně povede k tomu, že zmeškají zranitelnosti, které by méně informovaný útočník nalezl a zneužil.

Pentestování v grey box překlenuje rozdíl mezi testováním white a black box. Tím, že pentester má omezené informace o cílovém systému, pentesty simulují úroveň znalostí, kterých by hacker s dlouhodobým přístupem k systému dosáhl při svém prozkoumávání systému.

Dle typu aktiva, aplikace a zařízení

- pentesty mobilních aplikací — Pentest CheatSheet – Aplikace na Google Play; The mobile application penetration testing methodology
- pentesty webových stránek (aplikací) — Podrobte webové stránky analýze během pár minut | Drupal.cz; Web Application Penetration Testing: Steps, Methods, & Tools
- pentesty IoT, ICS/SCADA — Nástroj pro penetrační bezpečnostní testy IoT zařízení | TR instruments
- pentesty rozhraní API — How To Prepare For An API Pentest - Curl - White Oak Security
- pentesty sociálním inženýrstvím — Testy sociálním inženýrstvím (aec.cz); Testy sociálního inženýrství (systemonline.cz)

  Cílem testu praktikami sociálního inženýrství je ověřit chování zaměstnanců ve vztahu k interním předpisům organizace, odolnost vůči nejnovějším hrozbám sociálního inženýrství a dodržování zásad dobré bezpečnostní praxe. Je důležité, aby uživatelé byli na tyto testy připraveni prostřednictvím programů budování bezpečnostního povědomí.

  Cíle testování chování:
  - Práce s elektronickou poštou
  - Práce s přenosnými médii
  - Telefonická komunikace
  - Fyzická bezpečnost

  Testované vektory:
  - spamming
  - phishing
  - vishing
  - spear phishing

Infrastrukturní a síťové

- pentesty bezdrátových sítí [Penetrační testování bezdrátových sítí – Bak. práce, Jiří Danielka (upce.cz)]
  Bezpečnostní testování bezdrátových sítí je důležité tam, kde se ve větším měřítku používá bezdrátová síťová infrastruktura, která je součástí důvěryhodných sítí nebo slouží k provádění bezpečnostně citlivých operací.
  Cíle Wi-Fi testů: viditelnost wifi sítí, útoky na protokoly a hesla, falešné AP a klientské útoky.
- zátěžové testy odolnosti před DoS
- testovací phishingové kampaně

Dle metodologie

- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)
- Web Application Security Consortium Threat Classification (WASC-TC)
- Penetration Testing Execution Standard (PTES)
- Information Systems Security Assessment Framework (ISSAF)

Primární oblasti pentestů

- Confidentiality
- Authentication
- Authorization
- Availability
- Integrity
- Non-repudiation

Fáze procesu penetračního testování

Nástroje

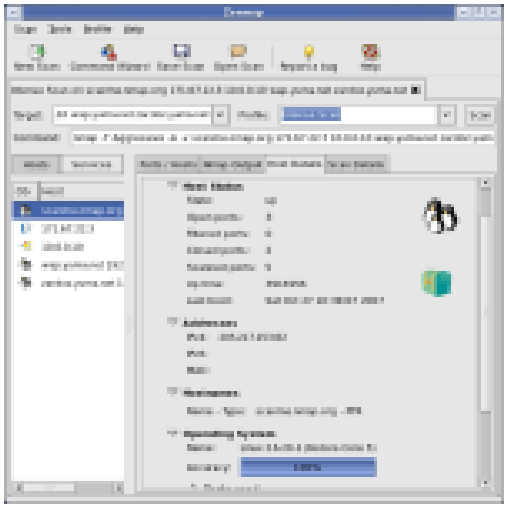
Online nástroje

Integra Czech Republic
Automated Penetration Testing | Intruder
Penetrační test online | zabezpecujeme.net
Agerit: Test bezpečnosti připojení k internetu (bezpecnosti.cz)
Pentest-Tools.com | Powerful Pentesting Tools, Easy to Use (pentest-tools.com)

Vlastní nástroje pentestera

Nástroje si každý pentester volí sám, stejně jako metodiky, na nichž zakládá postupy a hodnocení. Níže je jen pár příkladů nástrojů pro zjišťování vlastností prvků infrastruktury a zranitelností, testování zranitelností. Za zmínku stojí KALI Linux, distribuce, která byla od začátku vybavena i množstvím dalších testovacích nástrojů…

NMap

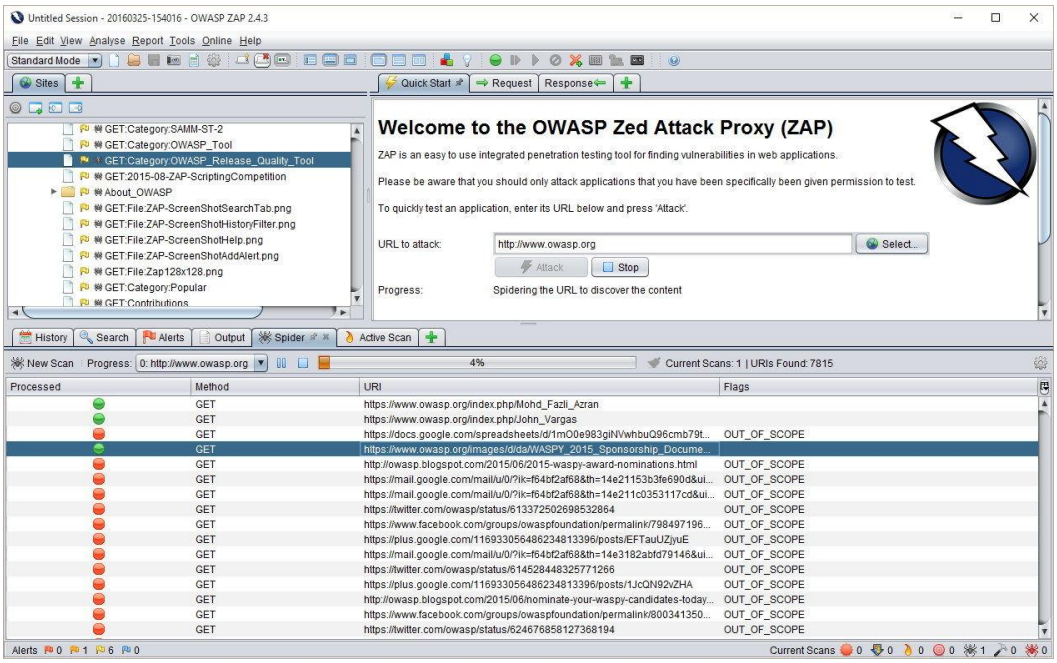


Nmap ("Network Mapper") je bezplatný a open source nástroj pro zjišťování sítě a audit zabezpečení. Mnoho systémů a správců sítě ji také považuje za užitečný pro úlohy, jako je inventarizace sítě, správu plánů upgradu služeb a sledování provozuschopnosti hostitele nebo služeb. Nmap používá raw pakety IP k určení, kteří hostitelé jsou v síti k dispozici, jaké služby (aplikace a verze) tito hostitelé nabízejí, jaké operační systémy (a verze) používají, jaký typ filtrů paketů na bráně firewall používá a pro desítky dalších charakteristik. Byl navržen pro rychlé skenování velkých sítí, ale funguje dobře i proti jednotlivým hostitelům.

KALI Linux

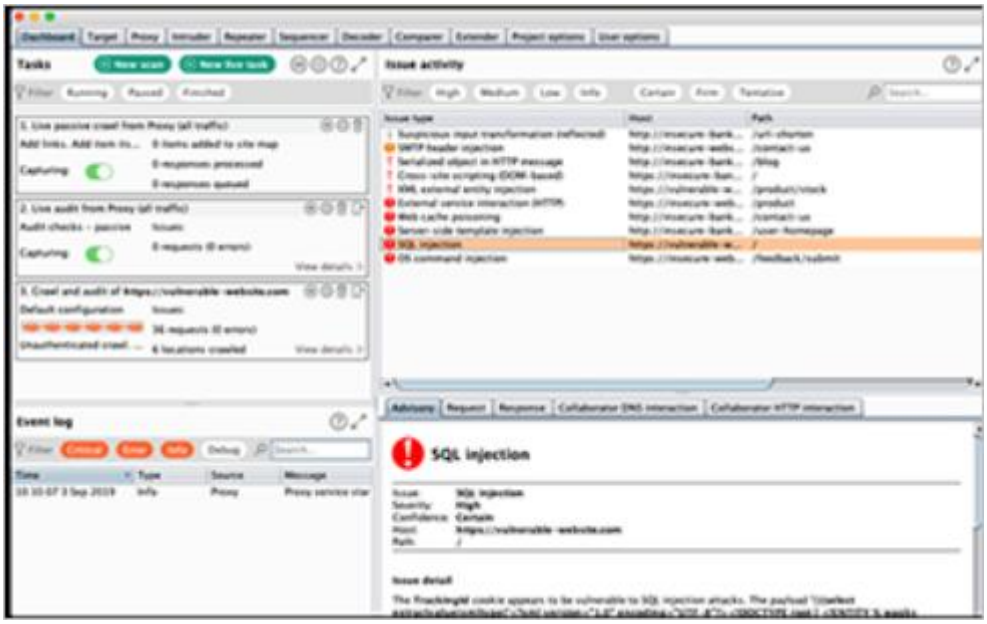
Kali Linux je linuxová distribuce založená na Debianu zaměřená na různé úkoly zabezpečení informací, jako je penetrační testování, bezpečnostní výzkum, počítačová forenzní analýza a reverzní inženýrství.

OWASP ZAP



Testování zabezpečení softwaru je proces posuzování a testování softwaru za účelem zjištění bezpečnostních rizik a zranitelností. Takové testování se dá dělat pasivním skenováním, aby se našly chyby zabezpečení. Nebo by to mohl být aktivní pentest, který simuluje uživatele se zlými úmysly, kteří se pokoušejí zaútočit na systém. Ve složitých systémech je obtížné ručně určit všechny možné chyby zabezpečení. Zed Attack Proxy (ZAP) je open source nástroj pro automatické hledání chyb zabezpečení ve webových aplikacích. Je to součást projektu OWASP. ZAP lze použít i jako prostředníka (proxy) mezi prohlížečem a aplikační serverem nebo samostatná aplikace nebo jako proces démona bez GUI. ZAP je vhodný pro zkušené bezpečnostní profesionály, webové vývojáře i funkční testery.

PortSwigger Burp



Existuje více edic Burpu: Enterprise, Proffessional a Community.

- Burp Suite Enterprise Edition je navržena tak, aby podporovala organizace a umožňovala automatizované skenování v celém jejich portfoliu.
- Více než 50 000 penetračních testerů a lovců odměn za chyby používá Burp Suite Professional, aby urychlili a zvýšili účinnost penetračního testování.
- Burp Suite Community Edition zpřístupní základy webového zabezpečení všem, aby pomohl vychovat další generaci bezpečnostních profesionálů.

Metasploit Framework

Dnes je Metasploit Framework považován za nejužitečnější nástroj pro auditování, který je volně dostupný odborníkům na zabezpečení a penetračním testerům. Má širokou škálu komerčních využití, prostředí pro vývoj exploitů a nástroje pro shromažďování síťových informací a pluginy pro zranitelnosti webových aplikací.

Metasploit Framework (MSF) poskytuje možnost spouštět exploity proti vybraným cílovým systémům a provádět úlohy simulující zneužití, jako je nahrávání souborů, spouštět procesy, vytváření síťových připojení přes zadní vrátka, monitorování používání systému a mnoho dalších. Proto je jeho primární použití v procesu penetračního testování.

Dalším důležitým využitím MSF je správa systémů. Vývoj exploitů byl dosud omezen na skupinu lidí v rámci bezpečnostních výzkumných, hackerských a testovacích komunit. S pomocí spolehlivé platformy, jako je Metasploit, mohou správci nyní zkontrolovat více serverů, zda nejsou ohroženy proti zneužití a mohou testovat zneužití, aby zjistili, zda jsou systémy skutečně zranitelné.

MSF má k dispozici mnoho různých rozhraní, z nichž každé má své silné a slabé stránky. Neexistuje žádné zaručeně dokonalé rozhraní pro použití s MSF, i když msfconsole je považována za jediný podporovaný způsob přístupu k většině funkcí MSF.

Kontext pro povinné osoby (nemocnice)

Jak řečeno dříve, povinné nemocnice mají některé povinnosti. Některé zvládnou samy, některé ne. A pro úvodní, možná i opakované (preventivní) skeny nabídl NÚKIB své služby.
Viz Zdroje níže:
NÚKIB - Jednou z forem preventivních aktivit je i penetrační testování. (nukib.cz)
Nicméně, CZ.NIC skeny webu nabízel donedávna všem st. organizacím a službu šlo objednat, jen byl trošku problém s kapacitami... Stejně tak prováděl i skeny dokumentových řešení a upozorňoval ty, kteří měli staré (zranitelné) verze WordPressu, Joomly apod.

Zdroje

Odkazy u položek a:

Offensive Hacks - YouTube
WiKi Security, PENETRATION TEST
IT Management - Penetrační testy
The Five Phases of Penetration Testing - YouTube
Jak si objednat pentest - kompletní návod - Citadelo
Testy zranitelností - Trusted Network Solutions (tns.cz)
An Overview of Penetration Testing (researchgate.net)
CSIRT.CZ nově provádí také penetrační testování - Root.cz
Nástroje pro penetrační testování: Vyberete si? | Computerworld.cz
Penetrační testování | Je vaše firma v bezpečí před hackery? (menzo.cz)
Security solutions to a leading Pharmaceutical Company | Sun Technologies
NÚKIB - Jednou z forem preventivních aktivit je i penetrační testování. (nukib.cz)
How to develop a structured approach to penetration testing - IT Governance UK Blog
What are Black Box, Grey Box, and White Box Penetration Testing? [Updated 2020] - Infosec
Nástroje pro penetrační testování webových aplikací a jejich praktické využití, Diplomová práce

Obsah