Vladimír Šulc

Penetrační testování – sociální inženýrství

Anotace: Penetrační testování ověřuje zabezpečení informačních systémů, sítí, aplikací a služeb, identifikuje zranitelnosti vůči možným útokům. Provádí se na základě dohody se zadavatelem jako nedestruktivní proces v určených termínech. Zranitelnosti lze analyzovat do detailu, ale jakékoli využití exploitů musí být předem schváleno.

Klíčová slova: penetrační testování, zranitelnosti, exploity, sítová infrastruktura, hrozby.

Úvod

Penetrační testy bezpečně napodobují útoky na specifické části infrastruktury zadavatele.[1] Na rozdíl od reálného útoku se tyto testy provádějí za předem definovaných podmínek, obvykle v kontrolovaném testovacím prostředí.[2] V závislosti na zvoleném režimu testování může mít auditor přístup k různým úrovním informací o testovaném systému. Penetrační testy se mohou zaměřit na různé úrovně, včetně perimetru (externí sítě), interních sítí nebo jednotlivých webových a mobilních aplikací, API a podobně.

Cílem každého penetračního testu je během stanoveného časového rámce identifikovat co nejvíce zranitelností, které by mohly být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům.[3] Na základě těchto nálezů se následně navrhují opatření k jejich odstranění.

Primárním účelem penetračního testu (pentestu) je identifikace bezpečnostních slabin v infrastruktuře organizace, softwarovém systému nebo aplikaci, které by mohly být potenciálně zneužity neoprávněným útočníkem. Jedná se o simulaci skutečného kybernetického útoku, při němž se testovací postupy flexibilně přizpůsobují na základě průběžně získávaných informací a zjištěných zranitelností.

Historicky byl pentest zaměřen na prokázání praktické využitelnosti zranitelností, často tím, že útočník pronikl do systému a provedl důkazní akci, jako například stažení citlivého souboru nebo úpravu dat.[4] V současnosti se však klade větší důraz na širokospektrální identifikaci co největšího počtu zranitelností, aniž by bylo nezbytné, aby všechny nalezené slabiny byly prakticky ověřeny nebo exploatovány.[5] Tento přístup s sebou však nese riziko falešných pozitivních výsledků, čímž může dojít ke záměně skutečného penetračního testu se samotným skenováním zranitelností, které často automatizovaně generuje seznamy potenciálních slabin bez hloubkové analýzy jejich skutečné exploitability.

V reakci na tuto situaci se stále častěji používají pokročilejší formy penetračních testů, jako jsou etický hacking (Ethical Hacking) nebo Red Teaming, které přesněji simulují komplexní útoky reálných hackerů, včetně použití sofistikovaných taktik, technik a procedur (TTP). Mezi nejrozšířenější veřejně dostupné metodiky, které slouží jako standardizované rámce pro provádění penetračních testů, patří OWASP Testing Guide (zaměřený na testování

---

1 MITNICK, Kevin D. a William L. SIMON. *Umění klamu: Jak chytrý hacker porazí váš firewall.* Přeložil Martin HERODEK. Brno: Computer Press, 2004.

2 OWASP Foundation. *OWASP Testing Guide v4*. OWASP, 2014. [online] [cit. 2024-09-19].

3 Národní ústav standardů a technologie (NIST). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. Gaithersburg: NIST*, 2008. [online] [cit. 2024-09-19].

4 HADNAGY, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley, 2011.

5 ALLSOPP, William. *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. Hoboken: Wiley, 2017.

bezpečnosti webových aplikací) a OSSTMM (Open Source Security Testing Methodology Manual), který pokrývá širší spektrum testovacích scénářů a aspektů bezpečnosti.

Kromě detekce běžně známých zranitelností, které lze objevit pomocí automatizovaných nástrojů pro skenování, je klíčovým přínosem penetračního testu schopnost odhalit i zcela nové, dosud neznámé slabiny (tzv. 0-day zranitelnosti). Tyto nově objevené slabiny často vyžadují kreativní a neautomatizovaný přístup, který jde daleko za rámec jednoduchého spuštění skenerů, a představují zásadní hrozbu, pokud zůstanou neodhalené a neopravené.

Režimy testování

Penetrační testy lze provádět ve třech různých režimech v závislosti na informacích a znalostech, které má tester k dispozici před zahájením testu:[6]

Black-box

Tester nemá k dispozici žádné informace o architektuře sítě, použitých technologiích ani jejich konfiguraci. Může se spolehnout pouze na specifikaci cílů (např. IP adresa, URL) a veškeré další informace musí získat z veřejně dostupných zdrojů.

Grey-box

Testerovi jsou poskytnuty základní informace o testovaném systému nebo aplikaci. Obvykle se jedná o údaje, které jsou dostupné legitimním uživatelům, včetně informací o architektuře sítě a použitých technologiích. Tento přístup zvyšuje šanci na odhalení většiny závažných zranitelností, zatímco stále zachovává riziko, že je skutečný útočník nenajde.

White-box

Tester má přístup k podrobným informacím o architektuře sítě, použitých technologiích a jejich konfiguraci, včetně znalosti bezpečnostní politiky organizace. Při testování webových aplikací má k dispozici také zdrojové kódy, popis API a veškerou potřebnou dokumentaci. Cílem je maximalizovat pravděpodobnost odhalení všech zranitelností, což vyžaduje úzkou spolupráci s administrátory a vývojovým týmem.

Postup testování

Penetrační testy se často provádějí v kombinaci s metodami etického hackingu a tzv. Red Teaming strategií, které se zaměřují na realistickou simulaci útoků.[7] Proces testování se skládá z šesti základních fází, přičemž každá z nich vyžaduje různou míru spolupráce ze strany zákazníka.[8] Doporučenou sedmou fází může být opakovaný test (re-test), který ověřuje účinnost přijatých nápravných opatření.

1. **Sběr informací**

   V úvodní fázi se provádí systematický sběr informací potřebných k vytvoření testovacích scénářů.[9] Tento krok se zaměřuje na hardwarová a softwarová aktiva, včetně lidských zdrojů, které by mohly hrát roli při možném narušení bezpečnosti. V rámci této fáze

---

6 OWASP Foundation. *OWASP Testing Guide v4. OWASP*, 2014. [online] [cit. 2024-09-19].

7 GRAGIDO, William a John PIRC. *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats.* Waltham: Syngress, 2011.

8 Národní ústav standardů a technologie (NIST). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. Gaithersburg: NIST*, 2008. [online] [cit. 2024-09-19].

9 OWASP Foundation. *OWASP Testing Guide v4. OWASP*, 2014. [online] [cit. 2024-09-19].

dochází především k aktivnímu skenování sítě, serverů a jiných prvků, s cílem identifikovat využívané služby.

2. **Hodnocení aktiv a identifikace cílů**

   Druhá fáze se soustředí na klasifikaci aktiv na základě různých kritérií, jako jsou operační systém, firmware, citlivost dat či otevřené porty. Kritická aktiva, která představují nejvyšší potenciální riziko, jsou prioritizována pro další testování. Na základě tohoto hodnocení se stanovují konkrétní cíle a scénáře pro penetrační testy.

3. **Identifikace zranitelností**

   Cílem této fáze je odhalení slabin v kritických systémech, které mohou být zneužity ke kompromitaci bezpečnosti, ať už ve formě neoprávněného přístupu, znepřístupnění služeb nebo manipulace s daty. Identifikace zranitelností se odvíjí od technologií používaných v prostředí zákazníka.[10] Automatizované nástroje jsou typicky využívány k nalezení známých zranitelností, přičemž je kladen důraz na správnou konfiguraci, bezpečnost přenosu citlivých dat a sílu šifrovacích a autentizačních schémat.

4. **Verifikace zranitelností a pokus o narušení bezpečnosti**

   Ve čtvrté fázi dochází k pokusu o zneužití identifikovaných zranitelností, jehož cílem je ověřit jejich praktickou vymahatelnost. Testy zahrnují například neautorizovaný přístup, eskalaci privilegií či znepřístupnění služeb. Tyto aktivity jsou prováděny s maximální opatrností, aby nedošlo k poškození testovaných systémů. Testování v této fázi nejen ověřuje nalezené zranitelnosti, ale také identifikuje další chyby, které automatizované nástroje neodhalily. Tester se pokouší zneužít odhalené zranitelnosti, přičemž využívá techniky pokročilé exploatace, které mohou zahrnovat multi-vektorové útoky nebo sociální inženýrství.[11]

5. **Hodnocení dopadů zneužití zranitelností**

   Po úspěšném útoku je nutné analyzovat, jaké dopady by mohla mít kompromitace bezpečnosti, včetně přístupu k datům, oprávnění a potenciálních možností další eskalace útoku.[12] Na konci této fáze jsou odstraněny všechny testovací účty a jakýkoli škodlivý či nestandardní kód, který byl v rámci testování nasazen.

6. **Tvorba závěrečné zprávy**

   Výsledkem celého procesu je podrobná závěrečná zpráva, která zahrnuje manažerské shrnutí, popis nalezených zranitelností a jejich dopadů. Zpráva obsahuje hodnocení rizik a doporučení k jejich mitigaci, včetně konkrétních návrhů na eliminaci nalezených slabin.

7. **Re-test**

   Po implementaci nápravných opatření je doporučeno provést re-test, jehož účelem je ověřit správnou implementaci těchto opatření a zjistit, zda při jejich realizaci nevznikly nové zranitelnosti. Tento krok je klíčový pro potvrzení celkové bezpečnosti systémů.

---

[10] Národní ústav standardů a technologie (NIST). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. Gaithersburg: NIST*, 2008. [online] [cit. 2024-09-19].

[11] Národní úřad pro kybernetickou a informační bezpečnost. *Případová studie NÚKIB: Spojenectví proti sofistikovanému zločinu.* [online] 2018.

[12] Národní ústav standardů a technologie (NIST). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. Gaithersburg: NIST*, 2008. [online] [cit. 2024-09-19].

Sociální inženýrství v penetračních testech

Penetrační testy zaměřené na odolnost uživatelů vůči technikám sociálního inženýrství se soustředí na praktickou prověrku jejich znalostí a povědomí o informační bezpečnosti.[13] Primárním účelem těchto testů je posoudit, jak uživatelé reagují na simulované útoky, aniž by byly přímo testovány technické systémy.[14] Důraz je kladen na to, zda uživatelé podlehnou útoku, nebo projeví obezřetnost. Kombinace psychologických a technických prostředků umožňuje testerům získávat citlivé informace, data nebo přístupové zdroje.

E-mailový test – Phishing

Cílem tohoto testu je prověřit, jak dobře jsou uživatelé připraveni čelit phishingovým útokům.[15] Na vybrané e-mailové adresy jsou odesílány podvodné zprávy, vytvořené na základě předem schválených scénářů. Tyto scénáře, přizpůsobené konkrétním požadavkům, mohou obsahovat odkazy na škodlivé weby či přiložené soubory simulující malware, s cílem vyvolat nebezpečnou akci nebo získat citlivé informace.

Telefonický test – Vishing

Vishingový test je založen na využití telefonních čísel, která mohou být veřejně dostupná na internetu,[16] poskytnutá zadavatelem testu, nebo získaná přímo testerem. Cílem podvodných telefonátů je přesvědčit uživatele k odhalení citlivých informací nebo k provedení nebezpečné akce, například spuštění aplikace, která simuluje škodlivý software.[17]

Cílený test – Spear phishing

Spear phishing představuje vysoce cílený phishingový útok, zaměřený na specifické jednotlivce,[18] jako jsou vrcholoví manažeři nebo správci domén. Tito jedinci mají potenciál výrazně ovlivnit bezpečnost celé organizace. Test zahrnuje důkladnou analýzu cíle, na jejímž základě je připraven útok přizpůsobený konkrétním charakteristikám napadené osoby.

Aktivní test fyzické bezpečnosti

Tento test se zaměřuje na ověření fyzické bezpečnosti organizace.[19] Útočník se pokouší neautorizovaně proniknout do neveřejných prostor organizace. Pokud se průnik podaří, test pokračuje snahou získat přístup k informačním systémům, pracovním stanicím nebo jiným citlivým zdrojům.

Pasivní test fyzické bezpečnosti

V rámci tohoto testu jsou na různých místech organizace strategicky umístěny USB disky obsahující škodlivý kód.[20] Sleduje se reakce uživatelů na jejich nález – zda disk správně označí za potenciální hrozbu a postupují podle interních směrnic, nebo zda se pokusí zařízení připojit k počítači a prozkoumat jeho obsah, čímž by mohli iniciovat škodlivý software.

---

[13] Národní úřad pro kybernetickou a informační bezpečnost. *Sociální inženýrství*. [online] 2016 [cit. 2024-09-19].

[14] MITNICK, Kevin D. a William L. SIMON. *Umění klamu: Jak chytrý hacker porazí váš firewall*. Přeložil Martin HERODEK. Brno: Computer Press, 2004.

[15] OWASP Foundation. *OWASP Social Engineering Framework. OWASP*, 2016. [online] [cit. 2024-09-19].

[16] Národní úřad pro kybernetickou a informační bezpečnost. *Sociální inženýrství*. [online] 2016 [cit. 2024-09-19].

[17] OWASP Foundation. *OWASP Testing Guide v4. OWASP*, 2014. [online] [cit. 2024-09-19].

[18] OWASP Foundation. *OWASP Social Engineering Framework. OWASP*, 2016. [online] [cit. 2024-09-19].

[19] Národní úřad pro kybernetickou a informační bezpečnost. *Sociální inženýrství*. [online] 2016 [cit. 2024-09-19].

[20] OWASP Foundation. *OWASP Social Engineering Framework. OWASP*, 2016. [online] [cit. 2024-09-19].

Závěr

Penetrační testování zaměřené na sociální inženýrství představuje důležitý nástroj pro ověření bezpečnostního povědomí uživatelů[21] a jejich schopnosti reagovat na různé druhy útoků. Na rozdíl od tradičních technických testů se zde důraz klade na lidský faktor, který může být v mnoha případech klíčovým prvkem při narušení bezpečnosti. Uživatelé mohou být vystaveni phishingovým e-mailům, podvodným telefonátům, cíleným spear phishing útokům nebo fyzickým průnikům. Sociální inženýrství tak poskytuje cenný vhled do praktické odolnosti zaměstnanců vůči kybernetickým hrozbám a umožňuje organizacím posílit jejich bezpečnostní strategii jak na úrovni technologií, tak lidských zdrojů. Výsledky testů ukazují na slabá místa, která mohou být následně eliminována školením zaměstnanců nebo úpravou bezpečnostních směrnic.[22]

Literatura

ALLSOPP, William. *Advanced Penetration Testing: Hacking the World's Most Secure Networks.* Hoboken: Wiley, 2017. ISBN 978-1-119-37216-7.

GRAGIDO, William a John PIRC. C*ybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats*. Waltham: Syngress, 2011. ISBN 978-1-59749-613-1.

HADNAGY, Christopher. *Social Engineering: The Art of Human Hacking.* Indianapolis: Wiley, 2011. ISBN 978-0-470-63953-5.

MITNICK, Kevin D. a William L. SIMON. Umění klamu: *Jak chytrý hacker porazí váš firewall.* Přeložil Martin HERODEK. Brno: Computer Press, 2004. ISBN 80-251-0171-7.

Národní úřad pro kybernetickou a informační bezpečnost. *Případová studie NÚKIB: Spojenectví proti sofistikovanému zločinu.* [online] 2018 [cit. 2024-09-19]. Dostupné z: https://www.cisco.com/c/dam/global/cs_cz/about/case-studies/pdf/case_study_nukib.pdf

Národní úřad pro kybernetickou a informační bezpečnost. *Sociální inženýrství*. [online] 2016 [cit. 2024-09-19]. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/

Národní ústav standardů a technologie (NIST). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment*. Gaithersburg: NIST, 2008. [online] [cit. 2024-09-19]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication 800-115.pdf

OWASP Foundation. *OWASP Social Engineering Framework*. OWASP, 2016. [online] [cit. 2024-09-19]. Dostupné z: https://owasp.org/www-project-social-engineering/

OWASP Foundation. *OWASP Testing Guide v4.* OWASP, 2014. [online] [cit. 2024-09-19]. Dostupné z: https://owasp.org/www-project-testing/

Rada Evropské unie. *Kybernetická bezpečnost: sociální inženýrství*. [online] 2023 [cit. 2024-09-19]. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity/cybersecurity-social-engineering/

Keywords: penetration testing, vulnerabilities, exploits, network infrastructure, threats

---

[21] Národní úřad pro kybernetickou a informační bezpečnost. *Sociální inženýrství.* [online] 2016 [cit. 2024-09-19].

[22] Rada Evropské unie. *Kybernetická bezpečnost: sociální inženýrství*. [online] 2023 [cit. 2024-09-19].

Summary

Penetration testing is used to verify the level of security and identify vulnerabilities in information systems, network infrastructure, applications and services. This process is carried out non-destructively and based on an agreement with the client. Social engineering is a specific form of penetration testing that focuses on the human factor and tests users' resistance to manipulation techniques such as phishing, vishing and spear phishing. The aim of these tests is to find out how users react to attempts to fraudulently obtain sensitive information or access data. Physical security testing examines an organization's ability to resist unauthorized physical intrusions.

The results of these tests reveal weaknesses that can be eliminated by training employees or modifying security procedures. Thus, social engineering plays a key role in assessing the overall resilience of organizations to cyber threats.

Ing. Vladimír Šulc, Ph.D.
Katedra bezpečnosti a práva
AMBIS vysoká škola, a.s.
Lindnerova 575/1
180 00 Praha 8
Email: vladimir.sulc@ambis.cz
Telefon: +420 605 714 895

Recenzent: mjr. JUDr. Matej Kostrec, PhD.