2. Obsah

3. Preambule k bezpečnostním testu

Tento dokument tvoří zadání bezpečnostního testu definuje testovací metodiku a postupy včetně dohledu průběhu testu, zvládání mimořádných situací, výjimek a omezení, na které bude během testování brán zřetel. Dále slouží k oboustranné dohodě a potvrzení testu zranitelností.

Realizace testu bude probíhat s využitím automatizovaných nástrojů pro skenování zranitelností v ICT a OT technologiích a službách s následným manuálním ověřením, přičemž cílem je zmapování maximálního možného počtu potenciálních zranitelností a bezpečnostních slabin, které jsou důsledkem chybějících bezpečnostních záplat na známé zranitelnosti a/nebo nedostatečné konfigurace operačních systémů a aplikačního software.

Z důvodu citlivosti testování je potřebné zafixovat pravidla testu v tomto dokumentu takovým způsobem, aby test proběhl v předem definované formě a kvalitě, čímž se minimalizují případná rizika.

4. Základní informace o testu

4.1.Časový rámec testu

Časový harmonogram bezpečnostního testu organizace. bude upřesněn před zahájením testu.

4.2.Cíl a rozsah testů

Bezpečnostní test se bude skládat z:

- OSINT – vytěžení veřejně dostupných informací o klientovi
- Externího penetračního testu
- Interního penetračního testu
- Penetračního testu wifi a jiných bezdrátových sítí v prostorách a okolí klienta, pokud budou zjištěny
- Detekce reakce bezpečnostních mechanismů klienta

Testované prostředí bude zahrnovat:

- Infrastrukturu dosažitelnou ze sítě internet
- Infrastrukturu dosažitelnou z LAN sítě – IT a ICS sítě/protokoly a zařízení
- Infrastrukturu dosažitelnost v bezdrátovém pásmu 2,4, 5 a 6 Ghz

Cílem bezpečnostního testu bude ověřit zda:

- lze získat neoprávněný přístup ke službám/datům/systémům,
- lze neoprávněně modifikovat/zničit data procházející komunikační infrastrukturou nebo zpracovávaná/uložená na systémech,
- lze proniknout bezpečnostním prvky,
- lze získat autentizační údaje,
- lze zneužít infrastrukturu k útokům na sítě a služby třetích stran a
- existují zranitelnosti, které mohou vést k předchozím bodům.

Testování zranitelností bude realizováno v uvedených oblastech vždy s využitím aktuálních dostupných databází zranitelností a nedostatků v implementaci nebo konfiguraci jednotlivých technologiích:

- definovaného IP rozsahu,
- síťové infrastruktury,
- bezpečnostního prvku,
- HW serveru/pracovní stanice,
- virtualizační platformy,
- OS Microsoft Windows / OS Linux.

Cílem prověrky bude odhalení případných bezpečnostní slabin a navrhnout účinná opatření k jejich eliminaci včetně stanovení priorit při jejich realizaci. Bude využito kombinace více testovacích metod, které v maximální míře umožní posoudit úroveň zabezpečení všech komponent testovaného rozsahu informačního systému ze všech dostupných vektorů.

Provedený test bude realizován bez přístupu ke zdrojovým kódům aplikací, bez přístupových oprávnění běžného uživatele.

5. Metodika testu

Kapitola obecně popisuje realizaci jednotlivých fází bezpečnostního testu v režimu „black-box“ a „gray-box“, což znamená, že provádíme test z prostředí sítě Internet přesně tak, jak by to činili kybernetičtí zločinci, případně s omezeným množstvím informací a součinnosti testované organizace. Realistický scénář útoku tak testuje nejen technickou připravenost, ale i lidský faktor v kontextu kybernetické bezpečnosti testované organizace.

5.1. Penetrační test

5.1.1. Fáze získávání informací

V této fázi je simulováno chování útočníka a technik v počáteční fázi sběru informací o cíli kybernetického útoku s využitím OSINT (Open source intelligence) a analýza těchto informací, kdy tyto informace slouží k volbě vhodných technik v průběhu fáze enumerace zranitelností

Během fáze získávání informací jsou získány základní informace o testované aplikaci/IS. Fáze získávání informací je složena z několika samostatných částí, mezi které patří sbírání dat, získávání informací apod. K vyhledávaným informacím patří např.

- doménová jména,
- IP adresy,
- informace o ISP,
- vlastníci aplikací, IS a služeb,
- autoři webových aplikací,
- publikované příspěvky zaměstnanců odhalující používané technologie,
- nechtěně publikované informace,
- vazby mezi obchodními partnery apod.

Tato fáze probíhá bez přímého kontaktu s testovanou aplikací nebo IS.

5.1.2. Fáze skenování infrastruktury

Fáze skenování představuje neinvazivní způsob zkoumání testované aplikace/IS, která většinou probíhá na síťové a transportní vrstvě. Mezi základní získávané informace patří:

- otevřené, zavřené nebo filtrované síťové porty,
- informace o publikovaných službách,
- identifikace používaných OS,
- základní pravidla chování firewallů, případně ostatních bezpečnostních technologií,
- základní pravidla pro chování síťových technologií pro překlad adres, load balancing, apod.

Na základě informací získaných z této fáze je možné určit další postup provádění bezpečnostních testů, které jsou konzultovány s odpovědným zaměstnancem organizace.

5.1.3. Fáze zjišťování stavu systémů a aplikací

Na základě poskytnutých nebo zjištěných informací dochází v této fázi k volbě vhodných technik pro enumeraci známých zranitelností v testovaných technologiích nebo v jejich konfiguracích. Techniky jsou voleny takovým způsobem, aby byl minimalizován negativní dopad na testované technologie.

Tato fáze představuje výzkum identifikovaných zranitelností, slabin nebo nevhodných konfigurací a jejich ověřování na testované aplikaci/IS. K hlavním úkolům této fáze patří:

- určení typů aplikací, IS nebo služeb, které mohou být zranitelné,

- úroveň aplikování opravných balíků,
- seznam možných DoS útoků,
- seznam oblastí, které mohou být zabezpečeny pomocí pravidla Security through obscurity,
- seznam jmenných konvencí na poštovních serverech atd.

Pro získávání vhodných postupů nebo nástrojů na využití těchto zranitelností je možné použít zdroje z Internetu (např. WWW, FTP, IRC služby, Google atd.). Pokud je to nutné nebo vhodné, testeři připravují vlastní postupy a nástroje.

5.1.4. Fáze exploitace

Na základě informací a analýzy nalezených zranitelností jsou zvoleny vhodné techniky pro exploitaci nalezených zranitelností v souladu se stanovenými cíli penetračního testu. Může se jednat v závislosti na stanovených cílech a pravidlech penetračního testu pouze o „proof of concept“ pro prokázání nalezených zranitelností a/nebo se může jednat o prvotní fázi průniku s cílem simulovat chování útočníka ve fázi post-exploitace.

Během této fáze jsou využívány dostupné exploity na známé zranitelnosti v technologiích a jejich konfiguracích a v případě potřeby jsou tyto exploity našimi konzultanty modifikovány, aby byla zajištěna jejich funkcionalita v testovaném prostředí. V některých případech je realizován vývoj vlastních exploitů na nalezené zranitelnosti

5.1.5. Fáze post-exploitace

Tato fáze slouží po úspěšné exploitaci nalezených zranitelností zejména k simulaci chování útočníka po prvotním průniku do testovaného prostředí s cílem udržení přístupu do prostředí, eskalace privilegií a laterárního pohybu v rámci prostředí a případného získání přístupu mimo IT prostředí.

5.2.Testovací a hodnotící standardy

Metodiky pro bezpečnostní testování používané konzultanty jsou založeny zejména, nikoliv však výlučně, na následujících metodikách, které se řadí do kategorie “best practice” pro různé typy bezpečnostního testování napříč různými sektory:

- Open Source Security Testing Methodology Manual,
- The Open Web Application Security Project,
- NIST 800-115,
- Common Vulnerability Scoring System,
- Center for Internet Security Benchmarks,
- doporučení pro zabezpečení od jednotlivých technologických dodavatelů,
- a dalšími.

5.2.1. OSSTMM

Dodavatel využívá jako základ pro bezpečnostní testování (tedy včetně penetračních testů) uznávaný mezinárodní standard OSSTMM – Open Source Security Testing Methodology Manual.

Tato metodika byla vytvořena v Institute for Security and Open Methodologies – www.isecom.org a je neustále rozvíjena velkou skupinou profesionálních testerů a specialistů na bezpečnost informačních a komunikačních technologií (ICT).

Metodika OSSTMM pokrývá provádění penetračních testů v jakémkoliv prostředí, kdy tester má stejná práva jako běžný uživatel. Ověřením všech oblastí, které jsou definovány v OSSTMM, je v systému proveden kompletní penetrační test.

OSSTMM nepředepisuje formu ani hloubku prováděných testů. Metodika se soustředí na stanovení základních modelů testování, hlavních oblastí testů a způsobu prezentace zjištěných výsledků.

Metodika vychází OSSTMM a neustále je aktualizována tak, aby odpovídala dnes nejlepším používaným praktikám v oboru bezpečnosti ICT a testování bezpečnosti. Nejvýznamnější zdroje metodiky jsou:

- normy řady ISO/IEC 27000,
- OWASP (Otevřený standard pro testování webových aplikací – www.owasp.org),
- NIST (National Institute of Standards and Technology – www.nist.gov – pouze dokumenty týkající se testování, nastavování a provozování bezpečnosti ICT).

Metodika OSSTMM definuje doporučený rozsah prováděných testů. Pracovníci dodavatele, kteří se specializují na testování bezpečnosti, neustále rozvíjí, udržují a katalogizují rozsáhlou databázi znalostí a konkrétních postupů. Tyto postupy a znalosti se týkají všech nejpoužívanějších operačních systémů, aplikací, síťových protokolů a obecné teorie ICT.

5.2.2. OWASP

Při testování webových aplikací se vychází z metodik, které pochází z projektu OWASP (www.owasp.org – The Open Web Application Security Project). OWASP zahrnuje mnoho různých služeb, např. „OWASP Testing Guide“, „Guide to Building Secure Web Applications and Web Services”, dále OWASP TOP TEN projekt, testovací nástroje, „OWASP Web Application penetration checklist” a mnoho dalších.

Pro testování a prezentaci výsledků bezpečnostních testů webových aplikací je použito metodiky OWASP Testing Guide ve verzi 4.

Provádění Secure Code Review je realizováno podle OWASP Code Review Guide v2.

5.2.3. NIST Special Publication 800-115

Jako pomocná metodika pro organizování testování je využíváno doporučení NIST SP 800-115 v některých vybraných částech, konkrétně v:

- posouzení bezpečnosti informací, včetně politik, rolí a odpovědností, využívaných metodik a Technik,
- identifikaci cílů a jejich analýzu z hlediska potenciálních zranitelností včetně technik vyhledávání v síti a skenování zranitelností,
- ověřování existence zranitelných míst,
- koordinaci, hodnocení, analýzy a zpracování dat.

5.2.4. CVSS

Zjištěné zranitelnosti jsou hodnoceny podle významu. Pro tento účel je využíváno metriky CVSS (Common Vulnerability Scoring System), která je průmyslovým standardem pro ohodnocování závažnosti zranitelností v informačních systémech. Na rozvoj této metriky CVSS dohlíží Forum of Incident Response and Security Teams (FIRST). Aktuální a při hodnocení použitá metodika je ve verzi 3.1.

Metrika CVSS usnadňuje rozlišení kritických zranitelností od těch méně významných, čehož dosahuje ohodnocováním zranitelných míst na bodové stupnici od 0 do 10, přičemž 0 značí nízký stupeň a 10 naopak vysoký. Hodnocení samotné pak probíhá v několika krocích a je založeno na sérii měření orientovaných na různé skupiny charakteristik té které zranitelnosti.

Zranitelnosti identifikované během skenování zranitelností nebo penetračního testu jsou klasifikovány v souladu s metrikou CVSS BMG (CVSSv3 Base Metric Group - https://www.first.org/cvss/v3-1/). Tato

metrika ohodnocení je zvolena s ohledem na její celosvětovou akceptaci v bezpečnostní komunitě a poskytuje vyvážený pohled na celkovou klasifikaci zranitelností.

CVSS BMG zachycuje charakteristiky nalezených zranitelností v osmi základních metrikách, které jsou konstantní v čase a nezávislé na prostředí, kde je aplikace provozována.

Použití metrik CVSS umožňuje sledování trendů vývoje zranitelnost systémů, párování s riziky zjištěnými v rámci analýz rizik a dalšími informaci v rámci systémů pro podporu rozhodování bezpečnostního managementu, jako je společností NGSS provozovaná služba SMC (https://www.ngss.cz/sluzba/14-security-management-center).

5.3. Používané nástroje

Všechny používané nástroje splňují několik základních kritérií, které obecně zajišťují vyšší bezpečnost a důvěryhodnost prováděných testů a omezují rizika vznikající při testování produkčních systémů.

Všechny nástroje jsou důkladně testovány na vlastním polygonu s cílem ověřit jejich správné fungování, skutečně vykonávané funkce a možné dopady na testované i okolní části systému.

Všechny klíčové nástroje jsou analyzovány a kompilovány pracovníky dodavatele. Nástroje, u kterého toto není možné, jsou zvýšenou měrou testovány a používají se pouze pro detekční účely, a ne ve fázích vytváření nebo udržování přístupu do testovaného systému.

V případě potřeby použití speciálního kódu na využití existující slabiny (tzv. exploit) jsou vždy preferovány vlastní programy nebo ty, u kterých je možné provést kontrolu zdrojového kódu a otestovat jejich funkčnost na polygonu.

Většina uvedených nástrojů nemá žádný, nebo jen minimální škodlivý dopad na vlastní testované systémy. U nástrojů, kde existuje vyšší riziko, ale kde kvalita a přidaná hodnota nástroje nelze nahradit žádným bezpečnějším způsobem, je toto uvedeno. Použití těchto nástrojů je vždy plánováno na dobu, ve které nejsou produkční systémy příliš využívány.

Mezi hlavní nástroje využité v prostředí klienta patří:

- Nessus Professional,
- Hydra,
- Terrascan,
- Metasploit.

5.3.1. Informovanost testerů

Před zahájením testů lze zvolit postup, lišící se mírou informovanosti testera tak, aby se co nejvhodněji simulovala role potenciálního útočníka.

5.3.1.1. Black box

Před realizací skenování zranitelností nebo penetračního testu disponují naši konzultanti minimem informací o testovaných cílech, např. pouze IP adresou, URL atp. Tento typ testu je zejména vhodný pro případy simulace chování externího útočníka.

5.3.1.2. Gray box

Před realizací skenování zranitelností nebo penetračního testu disponují naši konzultanti omezenou sadou informací o testovaných cílech, např. architektuře, technologiích a uživatelích a zároveň základní přístupy k testovaným cílům, např. na úrovni legitimního uživatele. Tento typ je zejména vhodný pro případ simulace chování interního útočníka s limitovanou sadou informací a uživatelskými oprávněními.

5.3.1.3. White box

Před realizací skenování zranitelností nebo penetračního testu disponují naši konzultanti veškerými dostupnými informacemi o testovaných cílech, např. plná dokumentace, zdrojové kódy aplikací atp. Zároveň disponují přístupem k testovaným systémům na úrovni privilegovaných uživatelů. Tento typ je zejména vhodný pro testování, kdy je potřeba identifikovat maximální množství zranitelností včetně těch, které není možné identifikovat v průběhu testování formou black box nebo gray box testů.

5.4. Opatření pro minimalizaci rizik

Přestože skenování většiny současných technologií na výskyt zranitelností má žádný nebo minimální negativního dopad, nelze u některých technologií negativní dopad zcela vyloučit. Z důvodu minimalizace negativního dopadu volíme zejména tyto postupy:

- včasné upozorňování na technologie, které mají být předmětem skenování zranitelností a je u nich známé zvýšené riziko negativního dopadu a doporučení alternativního postupu enumerace zranitelností,
- nastavení automatizovaných nástrojů pro skenování zranitelností takovým způsobem, aby testování minimalizovalo potřebné zdroje na straně testovaných technologií,
- skenování zranitelností probíhá po dílčích částech,
- v případě, kdy je možné realizovat skenování zranitelností jako white box test, aniž by to negativně ovlivnilo výsledek realizovaného testu, doporučujeme vždy realizaci skenování zranitelností tímto způsobem,
- v případě, kdy je možné realizovat skenování zranitelností v testovacím prostředí, aniž by to negativně ovlivnilo výsledek realizovaného testu, doporučujeme vždy realizaci v testovacím prostředí,
- v případě zjištění, během provádění testů, že testovaná infrastruktura a aplikace byly v minulosti cílem útoku a byly tímto útokem kompromitovány, bude provádění testů přerušeno až do vyřešení vzniklého incidentu. Zástupce společnosti organizace bude o této skutečnosti neprodleně informován.

5.5. Závěrečná zpráva

Z bezpečnostního testu bude zpracována závěrečná zpráva v předpokládané následující struktuře (finální struktura může být testerem upravena tak, aby lépe odrážela výsledky testu).

- manažerské shrnutí zahrnující souhrn zjištění a doporučení k přijetí opatření s indikací prioritizace opatření,
- základní informace o testu včetně časového rámce, cílů, rozsahu, technických údajů, údajů o testovacím týmu, omezeních testu apod.,
- metodika testu popisující fáze testu i použité metriky tak, aby bylo možné test periodicky opakovat, případně ověřit výsledky,
- výsledky testu se statistickým vyhodnocením a podrobným popisem zjištěných nálezů v testovaném rozsahu systémů, sítí apod.

6. Parametry testu

6.1. Nastavení prostředí

Externí část testu bude probíhat vzdáleně ze systémů společnosti NGSS prostřednictvím veřejné sítě internet. Test wifi bude probíhat v prostorách klienta a v přilehlém okolí. Interní část testu bude provedena z LAN. Pro účely testu poskytne klient testerovi 1 IP adresu v segmentu uživatelských stanic.

Systémy testera provedou před zahájením testů časovou synchronizaci proti důvěryhodnému časovému zdroji.

Pro zařízení testerů jsou primárně vyhrazeny adresy 85.207.10.109 a 91.245.8.110, případně dle okolností testu i jiné.

6.2. Testovaný rozsah

Testované rozsahy si zajistí tester samostatně na základě OSINT.

Místní penetrační test bude probíhat primárně v lokalitě Smetanova 2401, 76001 Zlín.

6.3. Technické parametry a průběh penetračního testu

Technické parametry jsou s ohledem na prostředí stanoveny následovně:

- maximální počet současně otevřených spojení – 10,
- maximální počet současně testovaných systémů – 5,
- maximální počet současných testů na systém – 2.

6.4. Sledované hodnoty

6.4.1. Testující strana

Na straně testera budou všechny výsledky prováděných testů opatřeny časovým indexem a uloženy. Sledované výsledky jsou výstupy testovacích nástrojů nmap a nessus. Kompletní záznam síťové komunikace mezi systémem auditora a testovaným systémem bude proveden nástrojem tcpdump a uložen ve standardním formátu pro následné zpracování analytickým nástrojem Ethereal.

6.4.2. Testovaná strana

Testovaná strana není vázána povinností sledovat průběh testu. Časovým indexem do standardních Systémových a Aplikačních logů uložené informace však mohou mít po skončení kampaně přidanou hodnotu pro zpětnou analýzu a rekonstrukci událostí.

6.4.3. Monitoring průběhu testu

V průběhu testu bude auditor neustále monitorovat dostupnost systému na úrovni ip stacku pomocí icmp dotazů. Vyhodnocována bude kromě existence odpovědí i jejich latence. Současně bude tester provádět dle jeho možností kontroly stavu testovaných aplikací.

Všechny uvedené hodnoty budou v případě zjištěných problémů s odezvou testovaných systémů uvedeny v dokumentu Závěrečná zpráva z testu.

6.5. Časový průběh testu

Následující časový harmonogram byl sestaven na základě empirických best-practice metod a dle možností organizace.

Čas T je časem přijetí závazné objednávky.

6.5.1. Interní test zranitelností

Testování bude zahájeno v do T+14 dní.

Předpokládané ukončení je do T+21 dní.

6.5.1. Zpráva z testu

Výsledná souhrnná zpráva z provedených testů bude klientovi předána do T+31 dní.

V případě úspěšného průniku nebo zjištění zásadní bezpečnostní slabiny bude informován odpovědný zástupce testované organizace a bude konzultován další postup testu.

6.6. Přístupové údaje

Přístupové údaje nebudou poskytnuty.

6.7. Komunikační scénář a dohled testovacího prostředí

Test zahájí tester na základě explicitního svolení odpovědné osoby organizace. Toto svolení odpovědná osoba vydává v okamžiku, kdy test prováděný podle této metodiky nemůže negativně ovlivnit fungování organizace

Organizace po celou dobu testu provádí aktivní monitoring systémů a odpovídající části síťové infrastruktury.

V případě události ovlivňujících chod testovaného systému odpovědná osoba neprodleně informuje testera a po vzájemné dohodě v testu pokračují nebo test ukončí.

V případě události ovlivňující vetší množství systémů, produkční systémy nebo významnou část infrastruktury informuje odpovědná osoba testera o této události a zahájí postup podle odpovídajících havarijních plánů. Tester okamžitě testování ukončí.

Po ukončení testování tester informuje odpovědnou osobu o ukončení testu. Odpovědná osoba provede kontrolu systému. V případě technických problémů provede odpovídající havarijní plán nebo plán obnovy.

6.7.1. Riziko infekce škodlivým kódem

Testovací postupy nepředstavují kybernetické riziko (nejsou nositeli škodlivého kódu) a proto není potřeba provádět před spuštěním dodatečná přípravná opatření spojená s ochranou před škodlivým kódem.

6.7.2. Riziko úniku citlivých dat

Práce s daty z průběhu kampaně (uživatelské údaje jako jméno, příjmení, IP adresa, email, pracovní pozice, závěrečná zpráva) bude striktně dodržovat zásady práce s citlivými údaji včetně GDPR regulace. Získané informace z kampaně budou odstraněny již v průběhu testování (např. získaná hesla nebudou ukládána celá, ale pouze částečně pro účel reportu apod.). Výjimky budou definované a uvedené v tomto dokumentu.