Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.0 | kyberbezpecnost@mirri.gov.sk | august 2023

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Návrh štandardov pre postupy pri penetračných testoch v prostredí verejnej správy

Obsah

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci, ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorený dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je pilotným výstupom v rámci Reformy Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

2 Úvod

2.1 Účel dokumentu

Účelom tohto metodického dokumentu pre penetračné testovanie je poskytnúť komplexný a systematický prístup k vykonávaniu penetračných testov v prostredí verejnej správy, či už vykonávaných interne alebo prostredníctvom externej služby. Dokument načrtáva kroky a postupy, ktoré sa budú dodržiavať počas procesu penetračného testovania, vrátane jeho cieľov a výstupov.

Hlavnými cieľmi tohto dokumentu sú:

- Poskytnúť jasnú a štruktúrovanú metodiku vykonávania penetračného testovania.
- Zabezpečiť, aby sa všetky aktivity penetračného testovania vykonávali konzistentným a opakovateľným spôsobom.
- Poskytovať usmernenia a osvedčené postupy na vykonávanie penetračného testovania spôsobom, ktorý je v súlade s priemyselnými normami a predpismi.

Tento metodický dokument je navrhnutý tak, aby ho mohli používať profesionáli v oblasti bezpečnosti, penetrační testeri a organizácie ako referenciu na plánovanie, vykonávanie a podávanie správ o aktivitách penetračného testovania. Jeho cieľom je podporiť spoločné chápanie účelu a cieľov penetračného testovania a poskytnúť štandardný prístup na vykonávanie penetračných testov. Rozsah penetračného testu bude definovaný a odsúhlasený organizáciou a penetračným testerom pred začatím testovania.

1.1 Definície a skratky

- API - Application Programming Interface
- CIISP - Chartered Institute of Information Security Professionals
- CREST - The Council for Registered Ethical Security Testers
- DDoS - Distributed Denial of Service
- DNS - Domain Name System
- DOM - Document Object Model
- DoS - Denial of Service
- HTTP - Hypertext Transfer Protocol
- IoT - Internet of Things
- ISACA - Information Systems Audit and Control Association
- ISO - International Organization for Standardization
- ISSAF - Information System Security Assessment Framework
- JMR - Jednotný metodický rámec
- MIRRI - Ministerstvo investícií, regionálneho rozvoja a informatizácie
- NCSC - National Cyber Security Centre
- NDA - Non-Disclosure Agreement
- NIST - National Institute of Standards and Technology
- OSINT - Open-source intelligence
- OSSTMM - Open Source Security Testing Methodology Manual
- OVM - orgány verejnej moci
- OWASP - Open Worldwide Application Security Project
- PENTEST – PENetračný TEST

- PTES - Penetration Testing Execution Standard
- RADIUS - Remote Authentication Dial-In User Service
- RFP - Request for Proposal
- SQL - Structured Query Language
- TACACS - Terminal Access Controller Access-Control System
- VS - Verejná správa
- XSS - Cross-Site Scripting

2. Východiskový stav

V súčasnej dobe neexistuje komplexné metodické usmernenie pre výkon penetračného testovania v prostredí verejnej správy.
Penetračné testovanie, tiež známe ako pentesting, alebo aj etický hacking, je technika posúdenia bezpečnosti, ktorá simuluje útok na systémy, aplikácie a siete organizácie s cieľom identifikovať slabé miesta a posúdiť účinnosť jej bezpečnostných opatrení. Uskutočnením pentestu môžu organizácie získať hlbšie pochopenie svojej bezpečnostnej situácie a identifikovať oblasti na zlepšenie.
Prínosy vykonania penetračného testu pre organizáciu sú početné a môžu mať významný vplyv na jej celkový bezpečnostný stav. Niektoré z kľúčových výhod zahŕňajú:

- Identifikácia zraniteľností - penetračný test môže odhaliť predtým neznáme zraniteľnosti, ktoré by mohli útočníci zneužiť. Tieto informácie umožňujú organizáciám určiť priority a riešiť bezpečnostné riziká skôr, ako môžu byť zneužité. Znalosť slabých miest, môže organizáciám pomôcť prijímať informované rozhodnutia o tom, kam prideliť zdroje na zlepšenie ich zabezpečenia.
- Vylepšený stav zabezpečenia - identifikáciou a odstránením slabých miest môžu organizácie zlepšiť svoju celkovú úroveň zabezpečenia a znížiť riziko úspešných útokov. Pravidelné penetračné testovanie môže organizáciám pomôcť udržať si náskok pred najnovšími hrozbami a zabezpečiť, aby ich bezpečnostné opatrenia zostali účinné.
- Overovanie súladu - penetračné testovanie môže organizáciám pomôcť overiť súlad s príslušnými bezpečnostnými štandardmi a predpismi. Toto môže byť obzvlášť dôležité pre organizácie v regulovaných odvetviach, pretože nedodržanie môže viesť k značným pokutám a iným vážnym následkom.
- Vylepšené schopnosti reakcie na incidenty - simuláciou útoku môže penetračný test pomôcť organizáciám identifikovať slabé miesta v procesoch a postupoch reakcie na incidenty a vykonať zlepšenia. To môže organizáciám pomôcť lepšie sa pripraviť na skutočné bezpečnostné incidenty a reagovať na ne, čím sa zníži dopad akéhokoľvek incidentu.
- Lepšie pochopenie hrozieb - penetračný test môže poskytnúť prehľad o typoch útokov a taktík, ktoré možno použiť proti organizácii, čo organizácii umožní lepšie pochopiť prostredie hrozieb a lepšie sa pripraviť na potenciálne útoky. To môže organizáciám pomôcť prijímať informovanejšie rozhodnutia o ich bezpečnostnej situácii a identifikovať oblasti, ktoré je potrebné zlepšiť.
- Zvýšené bezpečnostné povedomie a vzdelávanie v oblasti bezpečnosti - uskutočnenie penetračného testu môže zvýšiť povedomie o otázkach bezpečnosti medzi zamestnancami a zainteresovanými stranami a poskytnúť príležitosti na školenia a vzdelávanie. Zvyšovaním povedomia a poskytovaním školení môžu organizácie pomôcť zamestnancom, aby si viac uvedomovali bezpečnosť a boli lepšie vybavení na ochranu pred útokmi.
- Nákladová efektívnosť: V porovnaní s nákladmi spojenými s úspešným útokom môže byť vykonávanie pravidelných penetračných testov nákladovo efektívnym spôsobom, ako identifikovať a riešiť zraniteľné miesta pred ich zneužitím. Proaktívnym prístupom k bezpečnosti môžu organizácie znížiť celkové riziko úspešných útokov a minimalizovať potenciálny dopad akéhokoľvek incidentu.

Penetračný test môže poskytnúť cenné informácie a poznatky, ktoré môžu organizáciám pomôcť zlepšiť ich stav zabezpečenia a lepšie sa chrániť pred kybernetickými útokmi. Vykonávaním pravidelných

testov si môžu organizácie udržať náskok pred najnovšími hrozbami, zabezpečiť, aby ich bezpečnostné opatrenia zostali účinné, a byť lepšie pripravené na akékoľvek potenciálne bezpečnostné incidenty. Prínosy penetračného testovania sú nesporné a organizácie, ktoré investujú do pravidelných pentestov, pravdepodobne zaznamenajú výrazné zlepšenia v ich celkovej bezpečnostnej situácii a znížené riziko úspešných útokov.

2.2 Iné typy bezpečnostného testovania

2.2.1 Red teaming

Red teaming je typ bezpečnostného testovania, ktorý zahŕňa simuláciu útoku na systémy alebo siete organizácie s cieľom identifikovať slabé miesta. Na rozdiel od iných foriem bezpečnostného testovania, ako je penetračné testovanie, ktoré sa zameriava na identifikáciu a opravu špecifických zraniteľností, red teaming využíva holistický prístup k bezpečnostnému testovaniu tým, že sa pokúša napodobniť akcie skutočného útočníka.

Cieľom red teamingu je identifikovať slabé miesta v zabezpečení organizácie, ktoré nemusia byť zjavné pri iných typoch testovania bezpečnosti. Red teaming zvyčajne zahŕňa tím skúsených bezpečnostných odborníkov, ktorí používajú rôzne techniky, vrátane sociálneho inžinierstva, phishingu a narušenia fyzickej bezpečnosti, aby získali prístup k systémom a údajom organizácie.

Red teaming je vysoko kolaboratívny proces, ktorý zahŕňa úzku koordináciu medzi red teamom a bezpečnostnými a IT tímami organizácie. Red team zvyčajne úzko spolupracuje s bezpečnostným tímom organizácie na identifikácii potenciálnych zraniteľností a vývoji scenárov útokov. Počas skutočného testovania sa červený tím pokúsi prelomiť obranu organizácie pomocou rôznych metód a techník, zatiaľ čo bezpečnostný tím organizácie sa pokúsi útoky odhaliť a reagovať na ne.

Red teaming je vysoko efektívny spôsob, ako identifikovať slabé miesta v zabezpečení organizácie a môže pomôcť organizáciám vyvinúť efektívnejšie bezpečnostné stratégie. Simuláciou útoku môže red team poskytnúť cenné informácie o pripravenosti organizácie na zabezpečenie a pomôcť identifikovať oblasti, v ktorých sú potrebné zlepšenia zabezpečenia. Môže tiež pomôcť organizáciám vypracovať efektívnejšie plány reakcie na incidenty tým, že identifikuje slabé miesta v ich existujúcich procesoch reakcie na incidenty.

2.2.2 Blue teaming

Blue teaming je typ bezpečnostného testovania, ktorý zahŕňa simuláciu kybernetického útoku na systémy alebo siete organizácie s cieľom otestovať a zlepšiť obranné schopnosti organizácie. Na rozdiel od red teamu, ktorý sa zameriava na napodobňovanie akcií útočníka, blue team sa zameriava na hodnotenie existujúcej bezpečnostnej infraštruktúry a procesov organizácie, aby sa zabezpečilo, že sú efektívne pri odhaľovaní potenciálnych kybernetických hrozieb a reagovaní na ne.

Cieľom blue teamingu je identifikovať slabé miesta v bezpečnostnej infraštruktúre a procesoch organizácie a vyvinúť stratégie a procesy na zlepšenie ich zabezpečenia. Blue teaming zvyčajne zahŕňa tím skúsených bezpečnostných profesionálov, ktorí úzko spolupracujú s IT a bezpečnostnými tímami organizácie na identifikácii potenciálnych zraniteľností a vývoji efektívnych bezpečnostných stratégií.

Počas blue teamingu bezpečnostný tím zvyčajne použije rôzne nástroje a techniky na simuláciu rôznych kybernetických útokov, ako sú phishingové útoky, infekcie škodlivým kódom a útoky typu odmietnutia

služby. Tím následne vyhodnotí efektivitu bezpečnostnej infraštruktúry a procesov organizácie pri odhaľovaní a reagovaní na tieto simulované útoky. To môže zahŕňať analýzu protokolov a iných bezpečnostných údajov na identifikáciu potenciálnych indikátorov ohrozenia, ako aj vykonávanie penetračných testov na identifikáciu potenciálnych zraniteľností v systémoch a sieťach organizácie.

Blue teaming je vysoko kolaboratívny proces, ktorý zahŕňa úzku koordináciu medzi blue teamom a IT a bezpečnostnými tímami organizácie. Blue team zvyčajne úzko spolupracuje s bezpečnostným tímom organizácie na identifikácii potenciálnych zraniteľností a vývoji účinných bezpečnostných stratégií. Tím môže tiež spolupracovať s ostatnými zainteresovanými stranami v rámci organizácie, ako sú napríklad právne tímy a compliance tímy, aby sa zabezpečilo, že zabezpečenie organizácie je v súlade s regulačnými a právnymi požiadavkami.

2.2.3 Purple teaming

Počas purple teamingu red team a blue team spolupracujú na simulácii kybernetických útokov, pričom red team hrá úlohu útočníka a blue team hrá úlohu obrancu. Red team použije rôzne taktiky, techniky a postupy, aby sa pokúsil preniknúť cez obranu organizácie, zatiaľ čo blue team použije rôzne nástroje a techniky na odhalenie a reakciu na útoky.

Purple teaming je zvyčajne navrhnutý tak, aby bol vysoko interaktívny a kooperatívny, s častými brífingmi a diskusiami medzi red a blue tímami, aby sa prediskutovali výsledky cvičenia a identifikovali oblasti na zlepšenie. Cieľom je identifikovať slabé miesta v obrane organizácie a vyvinúť efektívnejšie stratégie a procesy na ich riešenie.

Purple teaming môže byť obzvlášť užitočný pre organizácie, ktoré predtým vykonávali red teaming a blue teaming oddelene, pretože môže pomôcť prelomiť komunikačné bariéry medzi týmito dvoma tímami a podporiť prístup k testovaniu bezpečnosti založený na väčšej spolupráci. Spoločnou prácou môžu red a blue tímy rýchlejšie a efektívnejšie identifikovať a riešiť zraniteľné miesta a vyvinúť robustnejšie a odolnejšie bezpečnostné procesy.

2.3 Aktuálna legislatíva VS

Legislatíva týkajúca sa penetračných testov
Na Slovensku sa penetračné testy riadia predovšetkým nasledovnou legislatívou:

- Zákon č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Zákon č. 45/2011 Z. z. Zákon o kritickej infraštruktúre

Prepojenie na ostatné výstupy v oblasti kybernetickej bezpečnosti
Návrh schémy nevyhnutných počtov obsadenia odbornými pozíciami v jednotlivých OVM a definovanie pracovných pozícií v oblasti kybernetickej bezpečnosti

- Dokument obsahuje popis schémy nevyhnutných počtov obsadenia odbornými pozíciami v jednotlivých orgánoch verejnej správy a definovanie pracovných pozícií v oblasti kybernetickej bezpečnosti vo verejnej správe (medzi pozíciami je aj tester kybernetickej bezpečnosti)

Metodika pre vznik odborných bezpečnostných pracovísk v prostredí verejnej správy

- Dokument obsahuje popis rôznych typov bezpečnostných pracovísk a metodiku na priradzovanie typov pracovísk ku kategórii OVM.
- Medzi kompetencia bezpečnostného pracoviska typu A patrí aj penetračné testovanie.

Jednotný metodický rámec (JMR)

- Cieľom metodického dokumentu – JMR je upraviť tvorbu a použitie riadiacich a podporných dokumentov pre implementáciu bezpečnostných opatrení v oblasti kybernetickej a informačnej bezpečnosti na úrovni OVM v súlade s platnou legislatívou, a tým zabezpečiť vyššiu efektívnosť plnenia bezpečnostných opatrení a zvyšovanie úrovne KIB v týchto organizáciách.

Definovanie technických a procesných nástrojov a postupov na splnenie bezpečnostného minima

- Metodické usmernenie pre implementáciu minimálnych bezpečnostných opatrení OVM pre oblasť kybernetickej a informačnej bezpečnosti.

Návrh etických štandardov pre sektor ITVS

- Dokument popisuje návrh etických štandardov pre sektor ITVS. Popisuje definovanie etických požiadaviek na zamestnancov a dané skupiny bezpečnostných expertov - požiadavky pri výbere a najímaní zamestnancov v daných roliach (interných ako ej externých).
- Ešte nie je dokončený.

Etické kódexy a audítorské štandardy pre penetračné testy v USA a Spojenom kráľovstve
V USA sa etické kódexy a audítorské štandardy pre penetračné testy riadia predovšetkým smernicami a nariadeniami stanovenými Národným inštitútom pre štandardy a technológie (NIST), Medzinárodnou organizáciou pre štandardizáciu (ISO) a Asociáciou Auditu a Kontroly Informačných Systémov (ISACA). Niektoré z kľúčových etických kódexov a štandardov pre penetračné testovanie v USA zahŕňajú:

- Špeciálna publikácia NIST 800-115: Táto publikácia poskytuje návod na vykonávanie penetračného testovania a hodnotenia zraniteľnosti v súlade s federálnymi požiadavkami pre bezpečnosť informačných systémov.
- ISO/IEC 27001: Táto norma poskytuje rámec pre systémy riadenia informačnej bezpečnosti vrátane požiadaviek na penetračné testovanie.
- Etický kódex ISACA: Etický kódex ISACA poskytuje návod na profesionálne správanie vrátane etických úvah pri vykonávaní penetračných testov a hodnotení zraniteľnosti.

V Spojenom kráľovstve sa etické kódexy a štandardy auditu pre penetračné testovanie riadia predovšetkým smernicami a nariadeniami stanovenými Národným centrom pre kybernetickú bezpečnosť (NCSC) a organizáciou Chartered Institute of Information Security Professionals (CIISP). Niektoré z kľúčových etických kódexov a noriem pre penetračné testovanie vo Veľkej Británii zahŕňajú:

- Rámec penetračného testovania NCSC: Tento rámec poskytuje návod na vykonávanie penetračného testovania v súlade s vládnymi normami a požiadavkami Spojeného kráľovstva.

- Kódex správania CREST pre penetračné testovanie: Tento kódex správania poskytuje etické pokyny na vykonávanie penetračných testov vrátane požiadaviek na transparentnosť, informovaný súhlas a rešpektovanie súkromia.

- Etický kódex CIISP: Etický kódex CIISP poskytuje návod na profesionálne správanie vrátane etických úvah pri vykonávaní penetračných testov a hodnotení zraniteľnosti.

Etické kódexy a audítorské štandardy pre penetračné testovanie sa môžu líšiť v závislosti od odvetvia, organizácie a krajiny. Pri vykonávaní penetračného testu je dôležité konzultovať štandardy a smernice špecifické pre dané odvetvie, ako aj právne a etické požiadavky.

2.4 Štandardy a postupy

Existujú rôzne metodiky vykonávania penetračných testov a tieto metodiky majú rôzne silné a slabé stránky. Jedným z dôvodov, prečo existujú rôzne metodológie pre penetračné testy, je to, že rôzne testy majú rôzne ciele. Niektoré testy sú určené na identifikáciu zraniteľností v systéme, zatiaľ čo iné sú určené na testovanie účinnosti bezpečnostných kontrol alebo na posúdenie súladu s predpismi. Napríklad hodnotenie zraniteľnosti môže byť vhodnejším prístupom, ak je primárnym cieľom identifikovať slabé miesta v systéme, zatiaľ čo audit súladu môže byť vhodnejší, keď je primárnym cieľom posúdiť súlad s predpismi.
Ďalším dôvodom, prečo existujú rôzne metodiky penetračných testov, je, že rôzne systémy vyžadujú rôzne prístupy k testovaniu. Napríklad webové aplikácie môžu vyžadovať manuálne testovanie alebo automatické testovanie pomocou špecializovaných nástrojov, zatiaľ čo sieťová infraštruktúra môže vyžadovať skenovanie zraniteľností, skenovanie portov a prelomenie hesla. Výber metodológie závisí od povahy testovaného systému a od typov zraniteľností, ktoré sa s najväčšou pravdepodobnosťou vyskytnú.

Úroveň prístupu udelená testerovi môže tiež ovplyvniť výber metodiky. Pri black-box testovaní nemá tester žiadne predchádzajúce znalosti o systéme, zatiaľ čo pri white-box testovaní má tester úplný prístup ku kódu a konfigurácii systému. Grey-box testovanie je kombináciou oboch. Úroveň prístupu udelená testerovi môže určiť použitú metodiku a to, či zahŕňa manuálne testovanie, automatizované nástroje alebo kombináciu oboch.
Zdroje, ktoré má organizácia k dispozícii, môžu tiež ovplyvniť výber metodiky. Niektoré metodiky môžu vyžadovať značné zdroje, ako je čas, odborné znalosti a špecializované nástroje. Organizácia by mala pri výbere metodiky zvážiť svoje zdroje a vybrať takú, ktorá je praktická a dosiahnuteľná.

Medzi najpoužívanejšie metodiky pre penetračné testy patria nasledovné:

- **Open-Source Security Testing Methodology Manual**

  Open Source Security Testing Methodology Manual (OSSTMM) je komplexná metodika na vykonávanie bezpečnostných testov a hodnotení. Poskytuje štruktúrovaný a systematický prístup k testovaniu bezpečnosti systémov, sietí a aplikácií. Metodológia OSSTMM pokrýva šesť fáz bezpečnostného testu, ktoré zahŕňajú:
  - Príprava - Definovanie rozsahu a cieľov bezpečnostného testu a získanie potrebných súhlasov a dohôd.

- Zhromažďovanie informácií - Zhromažďovanie informácií o cieľovom systéme, sieti a aplikáciách.
- Skenovanie - Vykonávanie automatizovaných skenov na identifikáciu potenciálnych zraniteľností a slabých stránok zabezpečenia.
- Testovanie - Hľadanie zraniteľností cieľového systému a pokus o ich zneužitie na získanie prístupu k citlivým údajom alebo systémom.
- Analýza - Posúdenie výsledkov bezpečnostných testov na určenie závažnosti zraniteľností a potenciálneho dopadu na cieľový systém.
- Tvorba správy - Zostavenie komplexnej správy o zisteniach a odporúčaniach na nápravu.

Metodológia OSSTMM je navrhnutá tak, aby bola flexibilná, čo umožňuje bezpečnostným testerom upravovať a prispôsobovať ju tak, aby spĺňala špecifické požiadavky ich testovacieho prostredia. Metodológia tiež poskytuje usmernenia pre dokumentáciu výsledkov a ich prezentáciu jasným a stručným spôsobom. Dodržiavaním OSSTMM môžu organizácie zabezpečiť, že ich úsilie o testovanie bezpečnosti bude dôkladné, presné a efektívne.

- **OWASP Web Security Testing Guide**

Testovacia príručka OWASP (Open Web Application Security Project) je komplexná metodika na vykonávanie bezpečnostných testov webových aplikácií. Poskytuje štruktúrovaný a systematický prístup k identifikácii a zmierňovaniu bezpečnostných rizík vo webových aplikáciách. Metodológia OWASP Web Security Testing Guide pokrýva nasledujúce fázy bezpečnostného testu:

- Zber informácií - zhromažďovanie informácií o cieľovej aplikácii alebo systéme. Zahŕňa to identifikáciu použitých technológií, mapovanie „attack surface“ a identifikáciu potenciálnych zraniteľností.
- Testovanie konfigurácie a správy nasadzovania - overiť, či je systém konfigurovaný bezpečne a že proces nasadenia bol správne implementovaný. Zahŕňa kontrolu použitia predvolených alebo slabých hesiel, nesprávne nakonfigurovaných serverov a zbytočných služieb, ktoré by útočníci mohli využiť.
- Testovanie správy identít - overenie toho, či systém dokáže správne spravovať identity používateľov. Zahŕňa to overenie, či funkcie registrácie používateľov, prihlásenia a riadenia účtu fungujú podľa očakávaní a že kontroly prístupu sa správne uplatňujú.
- Testovanie autentifikácie - overuje, že mechanizmy autentifikácie používané systémom sú bezpečné a nemožno ich ľahko obísť. Zahŕňa testovanie slabých hesiel, mechanizmov obnovenia hesla a ďalších zraniteľných miest súvisiacich s autentifikáciou.
- Testovanie autorizácie - zisťuje, či systém správne vynucuje kontroly prístupu a oprávnení. Zahŕňa testovanie eskalácie vertikálnych privilégií, horizontálnu eskaláciu privilégií a ďalších zraniteľných miest súvisiacich s autorizáciou.
- Testovanie správy relácií - overenie, či systém dokáže správne spravovať relácie používateľov a zabrániť útokom súvisiacim s reláciou. Zahŕňa testovanie na fixáciu relácií, únos relácie a ďalšie zraniteľné miesta súvisiace s reláciou.
- Testovanie validácie vstupu – overenie, či systém dokáže správne spracovať vstup používateľa a zabrániť zraniteľnostiam súvisiacim so vstupom, ako je napríklad vkladanie SQL výrazov, vkladanie príkazov OS, atď.

- Testovanie spracovania chýb - zisťuje, či systém dokáže správne zvládnuť chyby a výnimky bez toho, aby odhalil citlivé informácie alebo umožnil útočníkom zneužívať chybové stavy.
- Testovanie na použitie slabej kryptografie - Cieľom tohto testovania je overiť, či systém používa silnú kryptografiu na ochranu citlivých údajov, ako sú heslá, čísla kreditných kariet a ďalšie dôverné informácie.
- Testovanie biznis logiky – overenie toho, či biznis logika systému funguje podľa očakávaní a útočníci ju nemôžu manipulovať. Zahŕňa testovanie logických nedostatkov, identifikáciu zraniteľností typu „race condition“ a ďalších zraniteľností súvisiacich s biznis logikou.
- Testovanie na strane web klienta - testovanie sa zameriava na zraniteľné miesta, ktoré existujú na strane klienta web aplikácie, ako je vkladanie JavaScript kódu, obchádzanie validácie na strane klienta a zraniteľné miesta založené na DOM.

Dodržiavaním metodológie OWASP Web Security Testing Guide môžu organizácie zabezpečiť, aby ich úsilie o testovanie bezpečnosti bolo komplexné, dôkladné a efektívne. Metodológia poskytuje pokyny na identifikáciu a zmiernenie bezpečnostných rizík vo webových aplikáciách a na dokumentovanie a reportovanie výsledkov bezpečnostných testov.

- **NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)**

NIST SP 800-115 je komplexná metodika na vykonávanie testov a hodnotení informačnej bezpečnosti. Poskytuje štruktúrovaný a systematický prístup k hodnoteniu bezpečnosti informačných systémov, sietí a aplikácií. Metodológia NIST SP 800-115 pokrýva nasledujúce fázy bezpečnostného testu:

- Plánovanie a príprava - Definovanie rozsahu a cieľov bezpečnostného testu a získanie potrebných súhlasov a dohôd.
- Zber informácií - Zber informácií o cieľovom systéme, sieti a aplikáciách.
- Analýza hrozieb a zraniteľnosti - Identifikácia potenciálnych hrozieb a zraniteľností na základe zhromaždených informácií.
- Testovanie - Vykonávanie bezpečnostných testov na vyhodnotenie zraniteľnosti cieľového systému a na určenie potenciálneho vplyvu bezpečnostných rizík.
- Vyhodnotenie výsledkov - Analýza výsledkov bezpečnostných testov s cieľom určiť závažnosť zraniteľností a potenciálny dopad na cieľový systém.
- Tvorba správy - Zostavenie komplexnej správy o zisteniach a odporúčaniach na nápravu.

Metodológia NIST SP 800-115 poskytuje návod na výkon technických bezpečnostných testov a na dokumentovanie výsledkov a ich prezentáciu. Dodržiavaním NIST SP 800-115 môžu organizácie dosiahnúť, že ich testovanie bezpečnosti bude dôkladné, presné a efektívne. Metodológia je zosúladená s ďalšími bezpečnostnými štandardmi a usmerneniami NIST, čím poskytuje konzistentný a komplexný prístup k testovaniu a hodnoteniu informačnej bezpečnosti.

- **PTES (Penetration Testing Execution Standard)**

PTES je komplexná metodika na vykonávanie penetračných testov. Definuje štandardizovaný prístup k vykonávaniu, dokumentovaniu a reportovaniu výsledkov penetračného testu. Metodológia PTES zahŕňa sedem fáz penetračného testu, ktoré zahŕňajú:

- Príprava - Definovanie rozsahu a cieľov penetračného testu a získanie potrebných súhlasov a dohôd.
- Zber informácií - Zhromažďovanie informácií o cieľovom systéme, sieti a aplikáciách.
- Modelovanie hrozieb - Identifikácia potenciálnych hrozieb a slabých miest na základe zhromaždených informácií.
- Analýza zraniteľnosti - Analýza cieľového systému z hľadiska zraniteľností a posúdenie ich potenciálneho vplyvu.
- Zneužitie (Exploitation) - Pokus o zneužitie identifikovaných zraniteľností na získanie prístupu k citlivým údajom alebo systémom.
- Post-Exploitation - Vykonávanie činností, ako je krádež údajov, eskalácia privilégií alebo laterálny pohyb v rámci napadnutých systémov.
- Tvorba správy - Zostavenie komplexnej správy o zisteniach a odporúčaniach na nápravu.

PTES poskytuje štruktúrovaný a systematický prístup k penetračnému testovaniu, ktorý zabezpečuje, že sú pokryté všetky dôležité aspekty testu a že výsledky sú presné a spoľahlivé. Metodológia tiež poskytuje usmernenia pre dokumentáciu výsledkov a ich prezentáciu jasným a stručným spôsobom. Nasledovaním PTES môžu organizácie zabezpečiť, aby ich penetračné testovanie bolo efektívne a opakovateľné.

- **ISSAF (Information Systems Security Assessment Framework)**

ISSAF je komplexná metodika na vykonávanie penetračných testov a hodnotení bezpečnosti. Poskytuje štruktúrovaný a systematický prístup k hodnoteniu bezpečnosti informačných systémov, sietí a aplikácií. Metodológia ISSAF pokrýva nasledujúce fázy bezpečnostného testu:

- Plánovanie - Definovanie rozsahu a cieľov bezpečnostného testu a získanie potrebných schválení a dohôd.
- Zber informácií - Zber informácií o cieľovom systéme, sieti a aplikáciách.
- Analýza hrozieb a zraniteľnosti - Identifikácia potenciálnych hrozieb a zraniteľností na základe zhromaždených informácií.
- Testovanie - Vykonávanie bezpečnostných testov na vyhodnotenie zraniteľnosti cieľového systému a na určenie potenciálneho vplyvu bezpečnostných rizík.
- Vyhodnotenie výsledkov - Analýza výsledkov bezpečnostných testov s cieľom určiť závažnosť zraniteľností a potenciálny dopad na cieľový systém.
- Tvorba správy - Zostavenie komplexnej správy o zisteniach a odporúčaniach na nápravu.

Metodológia ISSAF poskytuje návod na vykonávanie bezpečnostných testov a na dokumentovanie výsledkov a ich prezentáciu jasným a stručným spôsobom. Metodológia tiež poskytuje návod na integráciu testovania bezpečnosti do celkového programu informačnej bezpečnosti a na meranie účinnosti testov bezpečnosti v priebehu času. Nasledovaním ISSAF môžu organizácie zabezpečiť, že ich úsilie o testovanie bezpečnosti bude dôkladné, presné a efektívne a že budú v súlade s osvedčenými postupmi.

3 Prehľad typov penetračných testov

Penetračné testovanie je cenným nástrojom na identifikáciu a riešenie slabých miest v systéme alebo sieti. Nie všetky penetračné testy sú však rovnaké a rôzne typy testov sú vhodnejšie pre rôzne scenáre. Tu je niekoľko dôvodov, prečo musíme pri výbere toho správneho zvážiť rôzne typy penetračných testov:

- Rôzne ciele - penetračné testy môžu mať rôzne ciele, ako je identifikácia slabín, testovanie účinnosti bezpečnostných kontrol alebo posúdenie súladu s predpismi. Typ zvoleného testu by mal byť v súlade so špecifickými cieľmi organizácie.
- Rôzne metodiky - metodiky penetračného testovania sa môžu značne líšiť, od black-box testovania , kde tester nemá žiadne predchádzajúce znalosti o systéme, po white-box testovanie, kde má tester úplný prístup ku kódu a konfigurácii systému. Zvolená metodika by mala byť vhodná pre testovaný systém a ciele testu.
- Rôzne úrovne prístupu - penetračné testy sa môžu líšiť aj úrovňou prístupu udeleného testerovi. Niektoré testy môžu povoliť iba externé testovanie z pohľadu neovereného používateľa, zatiaľ čo iné môžu poskytnúť úplný prístup do systému. Úroveň udeleného prístupu by mala byť primeraná cieľom testu a risk apetítu organizácie.
- Rôzne typy systémov - penetračné testy môžu byť zamerané na rôzne typy systémov, ako sú webové aplikácie, mobilné aplikácie alebo sieťová infraštruktúra. Pri výbere vhodného typu testu by sa mal brať do úvahy typ testovaného systému.
- Rôzne právne a etické úvahy: Penetračné testovanie môže vyvolať právne a etické obavy. Rôzne typy testov môžu mať rôzne právne a etické dôsledky a tieto by sa mali zvážiť pri výbere vhodného typu testu.

Výber správneho typu penetračného testu vyžaduje starostlivé zváženie konkrétnych cieľov, metodológie, úrovne prístupu, typu systému a príslušných právnych a etických úvah. Výberom vhodného typu testu môžu organizácie efektívnejšie identifikovať a riešiť zraniteľné miesta vo svojich systémoch a zlepšiť ich celkovú bezpečnostnú pozíciu.

3.1 Typy penetračných testov

3.1.1 Z hľadiska prístupu k testovaniu

Penetračné testovanie a red-teaming sú dve úzko súvisiace, ale odlišné spôsoby testovania bezpečnosti. Obe majú za cieľ posúdiť bezpečnosť cieľového systému, líšia sa však rozsahom, zameraním a cieľmi.

3.1.1.1 Penetračný test

Penetračné testovanie je simulovaný útok na cieľový systém na identifikáciu slabých miest a posúdenie bezpečnostného stavu systému. Cieľom penetračného testovania je identifikovať a zneužiť slabé miesta v systéme, poskytnúť odporúčania na nápravu a overiť účinnosť bezpečnostných kontrol. Penetračné testovanie zvyčajne zahŕňa kombináciu automatizovaných a manuálnych testovacích techník a zameriava sa na identifikáciu a zneužitie konkrétnych zraniteľností.

3.1.2 Z hľadiska pozície testera

Externé aj interné penetračné testy majú za cieľ posúdiť bezpečnosť cieľového systému simuláciou útoku. Hlavným rozdielom medzi nimi je však perspektíva, z ktorej sa test vykonáva.

3.1.2.1 Externý penetračný test

Externý penetračný test simuluje útok z miesta mimo siete organizácie a napodobňuje útočníka, ktorý má obmedzené alebo žiadne informácie o cieľovom systéme. Účelom tohto typu testu je posúdiť bezpečnosť systému z externého hľadiska, ako je napríklad webová aplikácia, ktorá je prístupná z internetu.

3.1.2.2 Interný penetračný test

Interný penetračný test simuluje útok zvnútra siete organizácie a napodobňuje útočníka, ktorý má interný prístup alebo znalosti, ako je napríklad súčasný zamestnanec, kontraktor alebo dodávateľ. Účelom tohto typu testu je posúdiť bezpečnosť systému z internej perspektívy, ako je podniková sieť alebo dátové centrum.

Externé aj interné penetračné testy môžu poskytnúť cenný pohľad na bezpečnostný stav systému, ale výber medzi nimi bude závisieť od bezpečnostných potrieb organizácie. Zatiaľ čo externý test poskytuje pohľad na bezpečnostnú situáciu zvonku, interný test poskytuje komplexnejší pohľad zvnútra siete organizácie.

3.1.3 Z hľadiska predbežných znalostí testera o cieli

3.1.3.1 Black-box test

Black-box test je typ penetračného testu, pri ktorom má tester obmedzené alebo žiadne informácie o cieľovom systéme. Tento typ testu simuluje útočníka, ktorý nemá žiadne predchádzajúce znalosti alebo informácie o cieľovom systéme, simuluje realisticky scenár, kde by útočník musel zbierať informácie a nájsť zraniteľné miesta pomocou prieskumu a iných techník. Účelom black-box testu je identifikovať a využiť zraniteľné miesta v cieľovom systéme a zároveň poskytnúť reálny pohľad na bezpečnostný stav systému z vonkajšej perspektívy. Tento typ testu sa často používa na posúdenie bezpečnosti webových aplikácií, sieťovej infraštruktúry a iných systémov, ku ktorým je možné pristupovať z internetu.

3.1.3.2 Gray-box test

Gray-box test je typ penetračného testu, pri ktorom má tester obmedzené znalosti alebo informácie o cieľovom systéme. Tento typ testu je navrhnutý tak, aby simuloval scenár, v ktorom má útočník nejaké informácie alebo prehľad o cieľovom systéme, ako je architektúra siete, IP adresy a ďalšie podrobnosti. Účelom gray-box testu je identifikovať a využiť zraniteľné miesta v cieľovom systéme a zároveň poskytnúť realistickejší pohľad na bezpečnostný stav systému. Tento typ testu sa často používa na posúdenie bezpečnosti interných systémov, ako sú podnikové siete, a poskytuje cielenejší a efektívnejší testovací proces ako black-box test. Tester môže mať prístup k internej dokumentácii, sieťovým diagramom alebo iným informáciám, ktoré mu môžu pomôcť lepšie pochopiť cieľový systém.

3.1.3.3 White-box test

White-box test je typ penetračného testu, pri ktorom má tester rozsiahle znalosti a informácie o cieľovom systéme. Tento typ testu simuluje útočníka, ktorý má interný prístup alebo znalosti, ako je napríklad súčasný zamestnanec, dodávateľ alebo kontraktor s prístupom do systému. Účelom white-box testu je identifikovať a využiť zraniteľnosti v cieľovom systéme a zároveň poskytnúť komplexný pohľad na bezpečnostný stav systému z internej perspektívy. Tento typ testu sa často používa na posúdenie bezpečnosti interných systémov, ako sú podnikové siete, a môže poskytnúť dôkladnejší a hlbší pohľad

na stav zabezpečenia systému ako iné typy penetračných testov. Tester môže mať prístup k zdrojovému kódu, konfiguráciám a ďalším citlivým informáciám, čo mu umožňuje testovať systém na hlbšej úrovni a identifikovať potenciálne bezpečnostné problémy, ktoré nemusia byť z externého hľadiska zrejmé.

3.1.4 Z hľadiska predmetu (target) testovania

3.1.4.1 Penetračné testovanie webových aplikácií

Penetračné testovanie webových aplikácií je typ hodnotenia bezpečnosti, ktorý sa zameriava na identifikáciu zraniteľností vo webových aplikáciách.
Prvým krokom v penetračnom teste webovej aplikácie je zhromaždenie informácií o webovej aplikácii vrátane technológie, na ktorej je postavená, jej funkčnosti a akýchkoľvek známych zraniteľnostiach. Tieto informácie sa používajú na vytvorenie mapy webovej aplikácie a na identifikáciu exponovaných bodov aplikácie.
Po zhromaždení informácií je ďalším krokom vykonanie identifikácia zraniteľností. To môže zahŕňať testovanie známych zraniteľností, ako je SQL injection alebo cross-site scripting (XSS), ako aj identifikáciu akýchkoľvek neštandardných konfigurácií, ktoré by mohol útočník zneužiť. Hodnotenie zraniteľnosti zahŕňa aj testovanie bezpečnosti autentifikácie a autorizácie webovej aplikácie, ako aj bezpečnosti komunikácie web aplikácie.
Po identifikácii zraniteľností je ďalším krokom vykonanie fázy exploitovania. V tejto fáze sa pentester pokúsi zneužiť slabé miesta a získať prístup k citlivým údajom alebo systémom, na ktoré sa webová aplikácia spolieha. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.2 Penetračný test infraštruktúry

Penetračný test infraštruktúry je hodnotenie bezpečnosti, ktoré sa zameriava na identifikáciu zraniteľností v sieťovej infraštruktúre organizácie vrátane serverov, sieťových prvkov a iných kritických systémov. Cieľom penetračného testovania infraštruktúry je zistiť, či útočník môže získať neoprávnený prístup k citlivým údajom alebo systémom prostredníctvom sieťovej infraštruktúry.

Prvým krokom pri penetračnom testovaní infraštruktúry je definovanie rozsahu hodnotenia vrátane systémov a sieťových komponentov, ktoré budú zahrnuté do testu. Ďalším krokom je vykonanie prieskumu a zhromažďovania informácií, ktoré môžu zahŕňať použitie nástrojov na mapovanie sieťovej infraštruktúry a identifikáciu potenciálnych zraniteľností.
Po dokončení fázy prieskumu a zhromažďovania informácií je ďalším krokom vykonanie samotného testovania. To môže zahŕňať pokusy o zneužitie zraniteľností v sieťovej infraštruktúre na získanie neoprávneného prístupu k citlivým údajom alebo systémom. Penetračné testovanie zahŕňa aj testovanie známych zraniteľností v operačných systémoch a aplikáciách.
Výsledky penetračného testovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.
To môže zahŕňať implementáciu opráv alebo aktualizácií na riešenie identifikovaných zraniteľností, implementáciu bezpečnostných kontrol na zabránenie neoprávnenému prístupu a aktualizáciu bezpečnostných politík a postupov.

3.1.4.3 Penetračný test siete

Penetračný test siete je testovanie bezpečnosti, ktoré sa zameriava na identifikáciu zraniteľností v sieťovej infraštruktúre organizácie. Cieľom sieťového penetračného testovania je zistiť, či útočník môže získať neoprávnený prístup k citlivým údajom, systémom alebo zdrojom v rámci siete. Tento typ testu

sa primárne zameriava na sieťové zariadenia ako napr. smerovače, prepínače, firewally, proxy servery a sieťové protokoly, ale aj podporné prvky ako napr. rôzne autentifikačné služby ako napr. TACACS a RADIUS.
Prvým krokom pri penetračnom testovaní siete je identifikácia rozsahu testu vrátane systémov, aplikácií a sietí, ktoré budú zahrnuté do hodnotenia. Tieto informácie sa používajú na vytvorenie mapy sieťovej infraštruktúry a na identifikáciu potenciálnych útočných plôch.

Po definovaní rozsahu je ďalším krokom vykonanie identifikácie zraniteľností. To môže zahŕňať identifikáciu otvorených portov, spustenie skenovania zraniteľností a analýzu konfigurácií siete z hľadiska slabých miest zabezpečenia. Hodnotenie zraniteľnosti môže zahŕňať aj testovanie známych zraniteľností v systémoch, aplikáciách a sieťach.

Keď sú zraniteľné miesta identifikované, ďalším krokom je pokúsiť sa ich zneužiť na získanie prístupu k citlivým údajom alebo systémom. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.4 Penetračný test mobilných aplikácií

Penetračné testovanie mobilných aplikácií je testovanie bezpečnosti, ktoré sa zameriava na identifikáciu zraniteľností v mobilných aplikáciách. Cieľom penetračného testovania mobilnej aplikácie je zistiť, či útočník môže získať neoprávnený prístup k citlivým údajom alebo systémom prostredníctvom mobilnej aplikácie.

Prvým krokom pri penetračnom testovaní mobilnej aplikácie je identifikácia rozsahu testu vrátane funkcií a vlastností, ktoré budú zahrnuté do hodnotenia.
Ďalším krokom je získanie kópie aplikácie. Môže to byť urobené stiahnutím aplikácie z online obchodu s aplikáciami alebo získaním aplikácie od vývojárskeho tímu.
Ďalším krokom je vykonanie testovania zabezpečenia aplikácie. To môže zahŕňať kontrolu bezpečnostných chýb v kóde aplikácie, testovanie používania šifrovania a bezpečných komunikačných protokolov a vyhodnotenie bezpečnosti ukladania a správy dát aplikácie. Kontrola zabezpečenia môže zahŕňať aj testovanie známych zraniteľností v operačnom systéme a platforme.

Po dokončení kontroly zabezpečenia je ďalším krokom vykonanie samotného penetračného testovania. Môže to zahŕňať pokusy o zneužitie zraniteľností v aplikácii na získanie neoprávneného prístupu k citlivým údajom alebo systémom. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.
.

3.1.4.5 Cloudové penetračné testovanie

Cloudové penetračné testovanie je hodnotenie bezpečnosti, ktoré sa zameriava na identifikáciu slabých miest v cloudových systémoch, aplikáciách a infraštruktúre. S rastúcim využívaním cloud computingu sa organizácie viac spoliehajú na cloudové systémy na ukladanie, spracovanie a správu citlivých údajov. V dôsledku toho je nevyhnutné posúdiť bezpečnosť týchto systémov, aby sa zabezpečila ich ochrana pred kybernetickými hrozbami.
Cloudové penetračné testovanie zvyčajne zahŕňa kombináciu manuálnych a automatických testovacích techník na posúdenie bezpečnosti cloudových systémov a aplikácií. To môže zahŕňať testovanie bezpečnosti základnej infraštruktúry, ako sú virtuálne stroje, úložné systémy a sieťové komponenty, ako aj testovanie bezpečnosti cloudových aplikácií a služieb.
Prvým krokom v penetračnom teste cloudu je zhromaždenie informácií o cloudovom prostredí vrátane

typu používaných cloudových služieb, typov údajov uložených v cloude a konfigurácií cloudových systémov a aplikácií. Tieto informácie sa používajú na vytvorenie mapy cloudového prostredia a na identifikáciu exponovaných miest.
Po zhromaždení informácií je ďalším krokom vykonanie posúdenia zraniteľnosti s cieľom identifikovať prípadné slabiny v prostredí cloudu. Môže to zahŕňať testovanie známych zraniteľností, ako je napríklad neaktualizovaný softvér alebo nesprávne nakonfigurované nastavenia zabezpečenia, ako aj identifikáciu akýchkoľvek neštandardných konfigurácií, ktoré by mohol útočník zneužiť.

Po identifikácii zraniteľností je ďalším krokom vykonanie fázy exploitovania, v ktorej sa pentester pokúsi zneužiť zraniteľnosti a získať prístup do cloudového prostredia. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.6 Penetračné testovanie API

Penetračné testovanie API (Application Programming Interface) je testovanie bezpečnosti, ktoré sa zameriava na identifikáciu zraniteľností v rozhraniach API, ktoré umožňujú komunikáciu medzi rôznymi softvérovými systémami. Rozhrania API zohrávajú kľúčovú úlohu pri umožňovaní komunikácie medzi aplikáciami a bežne sa používajú vo webových aplikáciách, mobilných aplikáciách a mikroslužbách.

Penetračné testovanie API zahŕňa testovanie bezpečnosti API a systémov, ktoré sa na ne spoliehajú. To môže zahŕňať testovanie známych zraniteľností, ako je SQL injection alebo cross-site scripting (XSS), ako aj testovanie bezpečnostných slabín v návrhu a implementácii API.

Prvým krokom v penetračnom teste API je zhromaždenie informácií o rozhraní API vrátane typov prenášaných údajov, metód používaných na prenos údajov a zavedených kontrol prístupu. Tieto informácie sa používajú na vytvorenie mapy API a na identifikáciu potenciálnych útočných plôch.

Po zhromaždení informácií je ďalším krokom vykonanie posúdenia zraniteľnosti s cieľom identifikovať akékoľvek slabé stránky v rozhraní API. Môže to zahŕňať testovanie známych zraniteľností, ako je napríklad neopravený softvér alebo nesprávne nakonfigurované nastavenia zabezpečenia, ako aj identifikáciu akýchkoľvek neštandardných konfigurácií, ktoré by mohol útočník zneužiť.

Po identifikácii zraniteľností je ďalším krokom vykonanie fázy exploitovania, v ktorej sa tester pokúsi zneužiť zraniteľnosti a získať prístup k API alebo systémom, ktoré sa na ňu spoliehajú. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.7 Penetračné testovanie bezdrôtových sietí

Penetračné testovanie bezdrôtových sietí je typ bezpečnostného hodnotenia, ktoré je zamerané na identifikáciu zraniteľností v bezdrôtových sieťach a zariadeniach. Bezdrôtové siete sa stávajú čoraz obľúbenejšími vďaka ich jednoduchému použitiu a mobilite, no prinášajú aj nové bezpečnostné riziká, ktoré je potrebné riešiť. Penetračné testovanie bezdrôtových sietí je navrhnuté tak, aby pomohlo organizáciám identifikovať a zmierniť tieto riziká.
Penetračné testovanie bezdrôtových sietí zvyčajne zahŕňa kombináciu manuálnych a automatických testovacích techník na posúdenie bezpečnosti bezdrôtových sietí a zariadení. To môže zahŕňať testovanie bezpečnosti bezdrôtových prístupových bodov, bezdrôtových klientov a základnej sieťovej infraštruktúry. Cieľom penetračného testovania bezdrôtových sietí je identifikovať zraniteľné miesta a

posúdiť riziko, ktoré tieto zraniteľnosti predstavujú. Dá sa to urobiť simuláciou útoku na bezdrôtovú sieť a vyhodnotením účinnosti zavedených bezpečnostných kontrol.

Prvým krokom v penetračnom testovaní bezdrôtových sietí je zhromaždenie informácií o bezdrôtovej sieti a zariadeniach, ktoré sú k nej pripojené. To môže zahŕňať identifikáciu používaných bezdrôtových protokolov, typ použitého šifrovania a prítomnosť akýchkoľvek bezdrôtových prístupových bodov. Po zhromaždení informácií je ďalším krokom vykonanie posúdenia zraniteľnosti s cieľom identifikovať akékoľvek slabé miesta v bezdrôtovej sieti. Môže to zahŕňať testovanie známych zraniteľností, ako sú slabé heslá alebo neaktualizovaný softvér, ako aj identifikáciu nesprávnych konfigurácií, ktoré by mohol útočník zneužiť.
Po identifikácii zraniteľností je ďalším krokom vykonanie fázy exploitovania, kde sa pentester pokúsi zneužiť zraniteľnosti a získať prístup k bezdrôtovej sieti. Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.8 Penetračný test metódou sociálneho inžinierstva

Pojem sociálne inžinierstvo sa vzťahuje na metódy používané útočníkmi na získanie dôvery koncového používateľa, aby útočník mohol získať informácie, ktoré možno použiť na prístup k údajom, systémom alebo fyzickým priestorom. Sociálne inžinierstvo zvyčajne zahŕňa predstieranie falošnej identity s cieľom manipulovať ľudí, aby poskytli informácie, ako sú heslá alebo osobné údaje.

Sociálne inžinierstvo môže zahŕňať telefónne hovory, e-maily alebo SMS. Sociálni inžinieri využívajú rôzne metódy, aby presvedčili používateľov, aby prezradili informácie, pričom sa často tvária ako technická podpora alebo zamestnanci organizácie.

Prvým krokom pri penetračnom teste metódou sociálneho inžinierstva je definovanie rozsahu testovania vrátane cieľových osôb, komunikačných kanálov, lokalít a fyzických priestorov, ktoré budú zahrnuté do testu. Ďalej sa pri testovaní obyčajne postupuje v nasledovných krokoch:

Prieskum cieľa - účelom sociálneho inžiniera je presvedčiť používateľa, že predstavuje dôveryhodnú osobu. Sociálni inžinieri sa často pokúšajú vytvoriť vzťah tým, že ponúknu ľahko dostupné podrobnosti, ako je dátum narodenia alebo telefónne číslo, ako dôkaz svojej legitimity. Mnohé z týchto informácií sú verejne dostupné a sociálni inžinieri zvyčajne skúmajú informačné zdroje z cieľovej organizácie, sociálne médiá a všeobecne internetové zdroje, aby zhromaždili tento typ zneužiteľných údajov.
Nadviazanie kontaktu s cieľom - útočník nadviaže priamy kontakt s cieľom. Sociálni inžinieri používajú informácie, ktoré zhromaždili, na overenie svojej falošnej identity. Cieľ je potom požiadaný, aby poskytol citlivé informácie, ktoré môže útočník zneužiť.
Exploitovanie (útok) - pomocou podrobností, ktoré takto získali, testeri vykonajú útok. To by mohlo zahŕňať prístup k systémom a dátam pomocou získaných hesiel, vykonanie klasického prípadu ukradnutia identity alebo využitie informácií pre získanie fyzického prístupu k priestorom a aktívam organizácie.
Výsledky fázy exploitovania sa používajú na vyhodnotenie rizika, ktoré vzniká na základe identifikovaných slabých miest a na vypracovanie odporúčaní na nápravu.

3.1.4.9 Penetračný test IoT (Internet of Things)

Penetračné testovanie internetu vecí (IoT) je proces hodnotenia bezpečnosti zariadení a systémov internetu vecí identifikáciou a využívaním zraniteľností. Cieľom penetračného testovania internetu vecí je identifikovať slabé miesta, ktoré by mohli útočníci zneužiť, a poskytnúť odporúčania na nápravu.

Prvým krokom v penetračnom teste internetu vecí je identifikácia rozsahu testu, ktorý zahŕňa zariadenia a systémy, ktoré budú testované, ako aj všetky obmedzenia testu. Tento krok je rozhodujúci, aby sa zabezpečilo, že test nenaruší normálnu prevádzku zariadení a systémov.

Ďalším krokom je vykonanie prieskumu na získanie informácií o zariadeniach a systémoch, ktoré budú testované. To zahŕňa identifikáciu typov zariadení, ich technickej špecifikácie, sieťovej topológie a operačných systémov a aplikácií, ktoré na nich bežia.

Následne sa testeri pokúsia identifikovať zraniteľné miesta v zariadeniach a systémoch. Dá sa to urobiť pomocou rôznych techník, ako je skenovanie zraniteľností, odposluch sieťovej komunikácie a manuálne testovanie.

Skenovanie zraniteľnosti zahŕňa použitie automatizovaných nástrojov na skenovanie zariadení a systémov na známe zraniteľnosti. Odposluch sieťovej komunikácie zahŕňa zachytávanie a analýzu sieťovej prevádzky s cieľom identifikovať komunikačné protokoly a potenciálne slabé miesta. Manuálne testovanie zahŕňa manuálne pokusy o zneužitie zraniteľností.

Ďalším krokom je zneužitie zistených zraniteľností. To zahŕňa pokus o získanie prístupu k zariadeniam a systémom využívaním ich zraniteľností. Cieľom tohto kroku je určiť rozsah škôd, ktoré by útočník mohol spôsobiť, ak by zneužil zraniteľné miesta.

Keď budú zraniteľné miesta zneužité, testeri zdokumentujú výsledky a poskytnú odporúčania na nápravu. Odporúčania môžu zahŕňať softvérové opravy, zmeny konfigurácie alebo implementáciu dodatočných bezpečnostných kontrol.

3.1.4.10 Testy na odmietnutie služby (DoS – Denial of Service)

Útok DoS (Denial-of-Service) je typ kybernetického útoku, ktorého cieľom je narušiť normálne fungovanie webovej stránky, sieťovej služby, servera alebo siete tým, že ich zahltí prevádzkou alebo požiadavkami na zdroje. Útok môže vykonať jednotlivec alebo skupina jednotlivcov pomocou siete počítačov, ktoré boli infikované škodlivým softvérom (BotNet).

Cieľom DoS útoku je zneprístupniť webovú stránku alebo server pre legitímnych používateľov spotrebovaním ich zdrojov, ako je šírka pásma alebo výpočtový výkon, do bodu, kedy už nebude môcť reagovať na legitímne požiadavky. Útok môže byť zameraný na konkrétne služby alebo protokoly, ako napríklad HTTP alebo DNS, s cieľom narušiť funkčnosť webovej stránky alebo ju úplne zneprístupniť.

V posledných rokoch sa DoS útoky vyvinuli do sofistikovanejších foriem, ako sú útoky DDoS (Distributed Denial-of-Service), ktoré využívajú sieť počítačov na zaplavenie webovej stránky alebo servera požiadavkami z veľkého počtu systémov, čo ešte viac sťažuje odrazenie útoku.

Útok DDoS (Distributed Denial-of-Service) je typ kybernetického útoku, ktorý je navrhnutý tak, aby zaplavil cieľový systém veľkým objemom prevádzky z viacerých zdrojov. Pri DDoS útoku útočník používa sieť kompromitovaných počítačov, známych aj ako botnet, aby zaplavil cieľový systém návštevnosťou. Botnet pozostáva z počítačov, ktoré boli infikované škodlivým softvérom alebo boli inak napadnuté a sú pod kontrolou útočníka.

Útoky DDoS sú mohutnejšie ako tradičné útoky DoS, pretože zahŕňajú veľké množstvo zdrojov, čo sťažuje cieľovému systému filtrovanie útokov. Útočná prevádzka môže pochádzať odkiaľkoľvek na

svete, čo sťažuje blokovanie alebo identifikáciu zdroja útoku.

DoS útoky sa zaraďujú primárne do nasledovných kategórií:

- Útoky založené na objeme komunikácie (volumetrické) - cieľom týchto útokov je zahltiť cieľový systém veľkým objemom prevádzky, ako sú záplavy cieľa UDP paketmi alebo záplavy cieľa ICMP paketmi.
- Protokolové útoky - útoky využívajúce slabé miesta v sieťových protokoloch, ako sú SYN floods alebo tzv. Smurf útoky.
- Útoky na aplikačnej vrstve - zameriavajú sa na aplikačnú vrstvu cieľového systému, pričom sa pokúšajú vyčerpať jeho zdroje alebo narušiť jeho funkčnosť. Príklady útokov na aplikačnej vrstve zahŕňajú napr. preťaženie HTTP požiadavkami a útoky typu DNS amplification.

3.2 Očakávané typy penetračných testov vo VS

Nasledujúca tabuľka zobrazuje očakávanú frekvenciu jednotlivých typov penetračných testov v prostredí verejnej správy:

Typ penetračného testovania	Odhadovaná frekvencia testov
Penetračné testovanie webových aplikácií	Vysoká
Penetračný test infraštruktúry	Stredná
Penetračný test siete	Nízka
Penetračný test mobilných aplikácií	Vysoká
Cloudové penetračné testovanie	Nízka
Penetračné testovanie API	Stredná
Bezdrôtové penetračné testovanie	Stredná
Penetračný test metódou sociálneho inžinierstva	Stredná
Penetračný test IoT (Internet of Things)	Nízka

Nasledujúca tabuľka uvádza približnú početnosť penetračných testov pre jednotlivé úrovne frekvencie testov:

Frekvencia testov	Približná početnosť testov v praxi
Nízka	Minimálne raz ročne
Stredná	Raz štvrťročne až polročne
Vysoká	Raz mesačne až štvrťročne

Konkrétne počty testov sú vždy špecifické pre konkrétnu organizáciu. Vychádzajú z rôznych faktorov,

ako ročný počet releasov, zmeny v technológiách organizácie, zmeny bezpečnostných trendov, hrozieb, rizík a frekvencii a veľkosti konfiguračných zmien počas roka.

4 Metodický postup a usmernenia pre realizovanie testov

V nasledujúcich kapitolách sú popísané kroky potrebné na vykonanie penetračného testu. Aj keď existujú rôzne metodiky vykonávania penetračných testov, existuje niekoľko všeobecných krokov, ktoré sa v procese zvyčajne dodržiavajú. Tieto kroky zahŕňajú napr. plánovanie a určenie rozsahu testu, zhromažďovanie informácií o cieľovom systéme alebo sieti, identifikáciu zraniteľností, exploitovanie zraniteľností a reportovanie zistení. Pochopením a dodržiavaním týchto krokov môžu organizácie vykonávať efektívnejšie penetračné testy a zlepšiť svoju celkovú bezpečnostnú pozíciu.

4.1 Fázy penetračného testovania

4.1.1 Definícia rozsahu a cieľov

Cieľ fázy

Táto kapitola definuje rozsah a ciele penetračného testovania, pričom uvádza, aké aktíva sa budú testovať, aký typ testovania sa bude vykonávať a aké ciele má testovanie dosiahnuť.

Popis fázy

Prvou fázou výkonu penetračného testovania s externou spoločnosťou je fáza definícia rozsahu. Táto fáza je rozhodujúca pre zabezpečenie toho, že ciele a očakávania penetračného testovania sú jasne definované a spoločnosť, ktorá bude vykonávať testovanie dokonale rozumie tomu, aké aktíva je oprávnená testovať.

Fáza definície rozsahu začína identifikáciou konkrétnych systémov, sietí, aplikácií a iných aktív, ktoré budú zahrnuté do penetračného testovania. Tento proces by mal byť založený na dôkladnom hodnotení rizík, ktoré identifikuje najkritickejšie aktíva organizácie a potenciálne hrozby a slabé miesta, ktoré by ich mohli ovplyvniť. Rozsah by mal zohľadňovať aj všetky regulačné požiadavky alebo zhody (compliance), ktoré musí organizácia dodržiavať.

Organizácia by tiež mala identifikovať potrebu vykonania penetračného testovania a cieľov, ktoré chce testovaním dosiahnúť. Typické ciele penetračného testovania zahŕňajú:

- Vyhodnotenie bezpečnosti systému alebo siete. Penetračné testovanie umožňuje organizáciám identifikovať a opraviť zraniteľné miesta skôr, ako ich môžu zneužiť útočníci.
- Preukázanie účinnosti bezpečnostných opatrení organizácie. Pravidelným vykonávaním penetračných testov môžu organizácie preukázať, že ich bezpečnostné opatrenia sú účinné pri ochrane pred kybernetickými útokmi.
- Poskytnúť základ pre budúce testovanie. Penetračné testovanie môže organizáciám pomôcť vytvoriť základnú líniu ich bezpečnostného stavu a sledovať zlepšenia v priebehu času.
- Zlepšiť celkovú bezpečnostnú pozíciu organizácie. Organizácie môžu zlepšiť svoju bezpečnostnú pozíciu identifikáciou a opravou slabých miest s následným znížením rizika úspešných útokov.
- Splnenie požiadaviek na súlad. Niektoré odvetvia majú regulačné požiadavky, ktoré nariaďujú pravidelné penetračné testovanie na zaistenie bezpečnosti citlivých informácií.

Výstupy fázy

- Popis rozsahu testovania.
- Popis cieľov penetračného testovania.

4.1.2 Identifikácia požiadaviek

Cieľ fázy

Táto kapitola uvádza nevyhnutné požiadavky na vykonávanie penetračného testovania, ako sú právne a regulačné požiadavky, technické požiadavky a obchodné požiadavky.

Popis fázy

Táto fáza zahŕňa identifikáciu špecifických požiadaviek na penetračné testovanie a stanovenie pravidiel zákazky pre spoločnosť, ktorá bude vykonávať testovanie.
Prvým krokom v tejto fáze je identifikácia špecifických požiadaviek na penetračné testovanie. To zahŕňa identifikáciu cieľov a účelu testovania, konkrétnych systémov a aplikácií, ktoré sa majú testovať, a typov zraniteľností, na ktoré sa testovanie zameria. Požiadavky by mali vychádzať z celkovej bezpečnostnej pozície organizácie a mali by byť v súlade so všetkými regulačnými požiadavkami alebo normami zhody, ktoré musí organizácia dodržiavať.
Po identifikácii požiadaviek je ďalším krokom stanovenie pravidiel zákazky pre externú spoločnosť. To zahŕňa vymedzenie rozsahu testovania, časového rámca testovania a špecifických testovacích metód, ktoré sa použijú.
Na zdokumentovanie požiadaviek a pravidiel zákazky by sa mal pripraviť dokument popisujúci požiadavky a pravidlá zákazky. Dokument by mal obsahovať nasledujúce informácie:

- Rozsah testovania – nadefinujú sa špecifické systémy a aplikácie, ktoré sa majú testovať, a všetky obmedzenia alebo výnimky.
- Ciele testovania - jasne sa nadefinujú ciele a zámery testovania a ako sú v súlade s celkovou bezpečnostnou pozíciou organizácie.
- Testovacie metodiky – uvedú sa konkrétne testovacie metodiky, ktoré sa budú používať počas výkonu zákazky
- Testovacie/produkčné prostredie – uvedie sa, či budú testy vykonané v produkčnom alebo testovacom prostredí. Určia sa všetky testovacie účty alebo poverenia, ktoré budú poskytnuté externej spoločnosti.
- Časový plán – návrh časového rámca pre testovanie vrátane akýchkoľvek termínov na podávanie správ a a prípadnú nápravu.
- Požiadavky na podávanie správ - popisujú požiadavky na ohlasovanie zraniteľností a poskytovanie odporúčaní na nápravu.
- Pravidlá zákazky - uvádzajú pravidlá pre výkon zákazky pre externú spoločnosť vrátane akýchkoľvek zakázaných činností alebo systémov.

Výstupy fázy

- Dokument popisujúci požiadavky a pravidlá zákazky

4.1.3 Výber externej spoločnosti

Cieľ fázy

Táto kapitola popisuje proces výberu externého dodávateľa, ktorý vykoná penetračné testovanie, vrátane hodnotenia jeho kvalifikácie, skúseností a reputácie.

Popis fázy

Táto fáza zahŕňa výber externej spoločnosti, ktorá má odborné znalosti a zdroje na efektívne vykonávanie testovania.

Prvým krokom v tejto fáze je vytvorenie zoznamu potenciálnych externých spoločností, ktoré by mohli vykonať testovanie. Môže to zahŕňať uskutočnenie online prieskum, vyžiadanie si odporúčaní od iných organizácií alebo kontaktovanie priemyselných združení.

Po vytvorení zoznamu potenciálnych externých spoločností je ďalším krokom vyhodnotenie schopností každej spoločnosti. To môže zahŕňať kontrolu ich webovej stránky, preskúmanie ich portfólia predchádzajúcej práce a vedenie rozhovorov s kľúčovými zamestnancami.

Pri hodnotení schopností každej spoločnosti je dôležité zvážiť faktory, ako sú:

- Odbornosť - Má externá spoločnosť potrebné odborné znalosti na efektívne vykonávanie testovania? Majú skúsenosti s testovaním typov systémov a aplikácií, ktoré budú testované?
- Zdroje - Má externá spoločnosť zdroje na vykonanie testovania v požadovanom časovom rámci? Majú potrebné hardvérové a softvérové nástroje?
- Reputácia - Aká je povesť externej spoločnosti v tomto odvetví? Dostali pozitívne recenzie od predchádzajúcich klientov?
- Súlad - Dodržiava externá spoločnosť príslušné normy a predpisy týkajúce sa súladu? Sú oboznámení so špecifickými požiadavkami organizácie na dodržiavanie predpisov?
- Cena - Aké sú náklady na testovanie? Je to v rámci rozpočtu organizácie?

Po vyhodnotení schopností každej externej spoločnosti by mala organizácia vypracovať užší zoznam potenciálnych kandidátov. Ďalším krokom je odoslanie žiadosti na predloženie ponuky (RFP) pre každú z užšie vybraných spoločností. RFP by mala obsahovať podrobnosti, ako sú požiadavky na testovanie, rozsah testovania a časový plán testovania. RFP by mala obsahovať aj zoznam hodnotiacich kritérií, ktoré budú použité pri výbere externej spoločnosti.

Po vydaní RFP budú mať externé spoločnosti stanovený časový rámec na odpoveď. Odpovede by mali obsahovať podrobnosti, ako je navrhovaný prístup k testovaniu, metodika, ktorá sa použije, a náklady na testovanie. Po prijatí odpovedí by mala organizácia vyhodnotiť každú odpoveď podľa hodnotiacich kritérií uvedených v RFP. To môže zahŕňať vedenie rozhovorov s externými spoločnosťami, preskúmanie ich predchádzajúcej práce a preskúmanie ich navrhovaného prístupu.

Po dokončení procesu hodnotenia by mala organizácia vybrať externú spoločnosť, ktorá najlepšie spĺňa požiadavky testovania. Organizácia by mala o svojom výbere informovať vybranú externú spoločnosť.

Výstupy fázy

- Zoznam potenciálnych externých dodávateľov a ich kvalifikácie.
- Užší zoznam externých dodávateľov, ktorí spĺňajú požiadavky organizácie.
- Žiadosť na predloženie ponuky (RFP)
- Výber externého dodávateľa.

4.1.4 Zmluvné a technické zabezpečenie penetračného testovania

Cieľ fázy

V tejto kapitole sú načrtnuté zmluvné aspekty, ktoré je potrebné zvážiť pri príprave zmluvy, ako aj technické zabezpečenie, ktoré by malo byť testerom poskytnuté..

Popis fázy

Zmluvné zabezpečenie

Pri príprave zmluvy na penetračné testy je potrebné zvážiť nasledovné:

- Súlad so zákonmi a predpismi - v zmluve by sa malo uvádzať, že externá spoločnosť musí dodržiavať všetky príslušné zákony a nariadenia súvisiace s penetračným testom, vrátane zákonov o ochrane údajov, zákonov o zneužití počítačov a akýchkoľvek predpisov špecifických pre dané odvetvie.
- Vlastníctvo údajov a duševného vlastníctva - zmluva by mala riešiť vlastníctvo údajov a duševného vlastníctva údajov vygenerovaných počas penetračného testu. Malo by špecifikovať, či si externá spoločnosť ponechá vlastníctvo akýchkoľvek nástrojov alebo techník použitých počas testu, alebo či sa vlastníctvo prevedie na organizáciu.
- Rozsah a obmedzenia - zmluva by mala jasne definovať rozsah penetračného testu a prípadné obmedzenia aktivít externej spoločnosti počas testu. Mala by tiež špecifikovať akékoľvek testovacie metódy alebo techniky, ktoré sú zakázané.
- Ukončenie a zrušenie - zmluva by mala obsahovať práva na ukončenie a zrušenie pre obe strany, vrátane požiadaviek na oznámenie a akýchkoľvek finančných pokút za porušenie zmluvy.

Právne a etické súvislosti - sú dôležitým aspektom penetračného testu, pretože zabezpečujú, že proces testovania prebieha zodpovedným spôsobom a v súlade s predpismi. Právne a etické hľadiská pomáhajú zabezpečiť, aby boli rešpektované práva jednotlivcov a organizácií a aby proces testovania nespôsobil škodu alebo neporušil žiadne zákony alebo nariadenia. Niekoľko bežných právnych a etických úvah pre penetračný test zahŕňa:

- Súlad s príslušnými zákonmi a nariadeniami - zabezpečenie toho, aby bol penetračný test v súlade s príslušnými zákonmi o ochrane osobných údajov, zákonmi o ochrane údajov a inými predpismi, ktoré sa môžu uplatňovať v jurisdikcii, v ktorej sa test vykonáva.
- Súhlas a autorizácia - získanie riadneho súhlasu a autorizácie od všetkých strán zapojených do penetračného testu, vrátane testovanej organizácie, jednotlivcov, ktorých informácie sa získavajú, a akýchkoľvek iných relevantných zainteresovaných strán.
- Ochrana údajov - zabezpečenie toho, aby sa s citlivými informáciami a osobnými údajmi zaobchádzalo a spracovávali bezpečným a zodpovedným spôsobom a aby boli zavedené vhodné bezpečnostné opatrenia na ochranu pred neoprávneným prístupom, zneužitím alebo krádežou informácií.
- Rešpektovanie práv jednotlivcov - rešpektovanie súkromia a bezpečnosti jednotlivcov, ktorých informácie sa získavajú počas penetračného testu, a zabezpečenie toho, aby sa všetky zhromaždené alebo spracované informácie použili len na účely testu.
- Zodpovednosť za neúmyselné následky - prevzatie zodpovednosti za akékoľvek neúmyselné dôsledky, ktoré môžu vyplynúť z penetračného testu, ako je výpadok systému alebo siete, a zabezpečenie prijatia vhodných opatrení na zmiernenie takýchto rizík.

Pri príprave zmluvy o poskytnutí penetračného testu je dôležité konzultovať s právny tímom, aby sa zabezpečilo, že všetky právne aspekty budú primerane vyriešené.

Dohoda o mlčanlivosti (NDA)

Dohoda o mlčanlivosti (Non-Disclosure Agreement) sa zvyčajne vyžaduje pred penetračným testom na ochranu dôvernosti citlivých informácií, ktoré môžu byť počas testu sprístupnené. Penetračné testovanie je proces identifikácie zraniteľností v systéme alebo sieti a testeri môžu počas svojej práce získať prístup k dôverným informáciám. To môže zahŕňať prihlasovacie údaje, osobné údaje, finančné údaje,

obchodné tajomstvá alebo iné citlivé informácie.

NDA zaisťuje, že penetrační testeri nemôžu zdieľať ani zverejňovať žiadne informácie, ktoré zhromaždia počas testu, a môže tiež špecifikovať rozsah a obmedzenia testovania. Podpísaním NDA sa penetrační testeri zaväzujú zachovať dôvernosť informácií a použiť ich len na účely penetračného testu. Pomáha to chrániť povesť organizácie a predchádzať možným právnym alebo finančným dôsledkom, ktoré by mohli vyplynúť z odhalenia citlivých informácií.

Autorizačný list
Autorizačný list sa zvyčajne vyžaduje pred penetračným testom na získanie výslovného povolenia od vlastníka alebo manažéra testovaného systému alebo siete. List dáva penetračným testerom zákonnú právomoc vykonať test a výslovne uvádza rozsah a obmedzenia testovania.
Penetračné testovanie zahŕňa aktívne skenovanie, odposluch sieťovej komunikácie a pokus o zneužitie zraniteľností v systéme alebo sieti. Bez predchádzajúceho povolenia by táto činnosť mohla byť považovaná za nezákonnú a viesť k občianskoprávnym alebo trestným postihom pre testerov a spoločnosť vykonávajúcu penetračný test.
Podpísaním autorizačného listu dáva vlastník alebo správca systému alebo siete výslovné povolenie na vykonanie penetračného testovania a tiež poskytuje dôležité podrobnosti, ako je rozsah, časový rámec a konkrétne systémy, ktoré sa majú testovať. To pomáha zabezpečiť, aby sa testovanie vykonávalo kontrolovaným a zodpovedným spôsobom, čím sa minimalizuje riziko narušenia obchodných operácií alebo neúmyselného poškodenia systémov.

Je dôležité poznamenať, že autorizačný list nenahrádza NDA, pretože tieto dva dokumenty slúžia na rôzne účely. Zatiaľ čo autorizačný list udeľuje povolenie na uskutočnenie testovania, NDA chráni dôvernosť citlivých informácií, ktoré môžu byť počas testu sprístupnené.

Technické zabezpečenie
Pred vykonaním penetračného testu by sa malo pripraviť alebo zvážiť niekoľko technických aspektov, aby sa zabezpečilo, že testovanie bude možné vykonávať efektívne. Niektoré z týchto technických aspektov zahŕňajú:

- Testovacie prostredie – v prípade interných testov, by pre testovací tím malo byť pripravené testovacie prostredie. To môže zahŕňať vyhradenú miestnosť alebo pracovný priestor s príslušným sedením. Testovací tím môže tiež vyžadovať prístup k samostatnej sieti alebo systému na účely testovania.
- Testovacie účty - testovacie účty by mali byť vytvorené pre testovací tím, aby ich mohol používať počas testovania. Tieto účty by mali mať príslušné povolenia a úrovne prístupu, ktoré umožnia testovaciemu tímu efektívne vykonávať testy.
- Káble, prepínače a iné vybavenie - testovací tím môže na vykonanie svojich testov vyžadovať prístup ku káblom, zariadeniam a nástrojom. To môže zahŕňať sieťové káble, USB disky a testovací softvér alebo hardvér.
- Prihlasovacie údaje - testovací tím môže vyžadovať prístup k prihlasovacím údajom, ako sú používateľské mená a heslá, na testovanie rôznych systémov a aplikácií. Tieto poverenia by mala poskytnúť organizácia a mali by byť dôverné.

Výstupy fázy

- Zmluva s externým dodávateľom
- Dohoda o mlčanlivosti (NDA)
- Autorizačný list

- Technické špecifikácie a požiadavky potrebné na vykonávanie penetračných testov.

4.1.5 Príprava plánu testov a komunikácie

Cieľ fázy

Táto kapitola pokrýva fázu prípravy a plánovania penetračného testovania, vrátane vypracovania plánu testovania a vytvorenia komunikačných kanálov so zainteresovanými stranami.

Popis fázy

Táto fáza zahŕňa prípravu harmonogramu testovania, ktorý pomáha zabezpečiť, aby sa testovanie vykonávalo efektívne a zároveň minimalizovalo akýkoľvek potenciálny vplyv na prevádzku organizácie.

Pri vývoji harmonogramu testovania je potrebné vziať do úvahy niekoľko faktorov:

- Ciele testu - plán testovania by mal byť navrhnutý tak, aby spĺňal ciele testu. Napríklad, ak je test zameraný na identifikáciu zraniteľností v konkrétnom systéme, plán testovania by mal byť navrhnutý tak, aby sa zabezpečilo dôkladné otestovanie všetkých komponentov tohto systému.
- Rozsah testu - Plán testovania by mal zohľadňovať aj rozsah testu. To zahŕňa identifikáciu systémov a aplikácií, ktoré budú zahrnuté do testu, ako aj typov zraniteľností, ktoré sa budú posudzovať. Plán testovania by mal byť navrhnutý tak, aby sa zabezpečilo, že všetky komponenty systému budú dôkladne testované v stanovenom časovom rámci.
- Dostupnosť zdrojov - plán testovania by mal zohľadňovať aj dostupnosť zdrojov. To zahŕňa dostupnosť testovacieho tímu, ako aj všetky potrebné nástroje alebo vybavenie. Plán testovania by mal byť navrhnutý tak, aby zabezpečil, že v prípade potreby budú k dispozícii všetky zdroje a že testovanie bude možné vykonávať efektívne.
- Časové obmedzenia - plán testovania by mal brať do úvahy aj akékoľvek časové obmedzenia, ktoré môžu byť prítomné. Napríklad, ak má organizácia prísny termín na dokončenie testu, plán testovania by mal byť navrhnutý tak, aby sa zabezpečilo, že test bude dokončený v tomto časovom rámci.
- Vplyv na prevádzku - plán testovania by mal zohľadňovať aj potenciálny vplyv na prevádzku organizácie. To zahŕňa identifikáciu všetkých kritických systémov alebo aplikácií, ktoré nemožno prepnúť do režimu offline na testovanie. Harmonogram testovania by mal byť navrhnutý tak, aby sa minimalizoval akýkoľvek potenciálny vplyv na prevádzku a zároveň by sa malo zabezpečiť dôkladné vykonanie testovania.

Po zohľadnení týchto faktorov je možné vypracovať plán testovania. Tento plán by mal obsahovať dátumy začiatku a konca testu, ako aj konkrétne časy dňa alebo dni v týždni, kedy sa testovanie uskutoční. Plán testovania by sa mal poskytnúť všetkým zainteresovaným stranám vrátane testovacieho tímu, projektového manažéra a akýchkoľvek iných relevantných strán.

Je potrebné tiež vypracovať komunikačný plán, ktorý je dôležitým aspektom penetračného testu, pretože načrtáva, ako budú informácie a výsledky zdieľané medzi všetkými zainteresovanými stranami zapojenými do procesu testovania. Dobre definovaný komunikačný plán pomáha zabezpečiť, aby boli všetci zladení a aby každý pochopil, čo od testu očakávať a kedy to očakávať. Typický komunikačný plán pre penetračný test obsahuje nasledujúce prvky:

- Zainteresované strany - zoznam všetkých jednotlivcov a tímov, ktorí sa zúčastnia penetračného testu, vrátane bezpečnostného tímu, IT tímu a vyššieho manažmentu.
- Úlohy a zodpovednosti - špecifické úlohy a zodpovednosti každého jednotlivca a tímu zapojeného do penetračného testu, vrátane toho, kto bude zodpovedný za plánovanie, vykonávanie a podávanie správ o teste.
- Plán - časový plán pre rôzne fázy penetračného testu vrátane plánovania a prípravy, testovania a podávania správ.
- Aktualizácie stavu - ako a kedy sa budú poskytovať aktualizácie stavu počas procesu testovania, vrátane pravidelných správ o pokroku a konečných výsledkov testov.
- Odstraňovanie alebo zmierňovanie zistení počas testov – akým spôsobom a kedy budú mitigované vybrané zistenia počas testu, akým spôsobom budú komunikované testerom zmeny, ktoré boli v prostredí vykonané a ako bude vyhodnocovaný vplyv mitigácií na výsledky a rozsah testu.
- Podávanie správ – návrh na formát a štruktúru záverečnej správy o teste vrátane toho, aké informácie budú zahrnuté a ako budú prezentované.
- Postupy eskalácie - Tu sú načrtnuté kroky, ktoré sa podniknú v prípade akýchkoľvek problémov alebo obáv počas procesu testovania, vrátane toho, koho kontaktovať a kedy eskalovať.

Výstupy fázy

- Plán testovania
- Komunikačný plán

4.1.6 Testovanie

Cieľ fázy

Táto kapitola pokrýva samotnú testovaciu fázu penetračného testovania, kde dodávateľ vykoná testovacie aktivity v súlade s plánom testovania.

Popis fázy

Táto fáza zahŕňa prieskum cieľa testovania a aktívne pokusy o zneužitie zraniteľností a získanie neoprávneného prístupu k cieľovému systému alebo sieti.
Po udelení prístupu externej spoločnosti začnú testovať definované systémy, aplikácie a siete. Testovanie by sa malo vykonávať podľa metodiky, ktorá bola načrtnutá v pláne testovania, a malo by zahŕňať kombináciu automatických a manuálnych testovacích techník.

Automatizované testovacie techniky môžu okrem iného zahŕňať skenovanie zraniteľností, mapovanie siete a skenovanie portov. Tieto techniky sa používajú na identifikáciu známych zraniteľností a potenciálnych vektorov útoku, ktoré by mohol zneužiť škodlivý aktér.

Manuálne testovacie techniky môžu zahŕňať prelomenie hesiel, sociálne inžinierstvo a využívanie zraniteľností, ktoré nemožno identifikovať pomocou automatizovaných testovacích techník. Tieto techniky sa používajú na identifikáciu slabých miest a vektorov útokov, ktoré sa nedajú identifikovať automatickým testovaním, a na testovanie účinnosti bezpečnostných kontrol a postupov.

Nasledujú všeobecné kroky, ktoré sa vykonávajú počas testovacej fázy penetračného testu:

- Prieskum - zozbieranie čo najväčšieho množstva informácií o cieľovom systéme alebo sieti. Dá sa to dosiahnuť vykonávaním techník pasívneho prieskumu, ako je zhromažďovanie informácií z otvorených zdrojov (OSINT) alebo aktívnym skenovaním cieľového systému alebo siete na získanie informácií.
- Skenovanie - aktívne skenovanie cieľového systému alebo siete s cieľom identifikovať všetky otvorené porty, služby alebo zraniteľné miesta, ktoré je možné zneužiť.
- Enumerácia - enumerácia systému alebo siete, aby sa zhromaždilo viac informácií, ako sú používateľské účty, heslá alebo akékoľvek iné citlivé informácie, ktoré možno použiť na získanie neoprávneného prístupu.
- Exploitovanie (Zneužitie) - po identifikácii zraniteľností a zhromaždení informácií sa penetračný tester pokúsi zneužiť zraniteľnosti na získanie prístupu k cieľovému systému alebo sieti.
- Post-Exploitation - po získaní prístupu sa penetračný tester pokúsi zachovať prístup do systému alebo siete a eskalovať privilégiá, aby získal prístup k citlivým údajom alebo zdrojom.

Testovacia fáza by sa mala vykonávať v kontrolovanom prostredí a len so súhlasom cieľovej organizácie alebo klienta, aby sa predišlo akýmkoľvek právnym alebo etickým problémom.

Počas testovania by mala externá spoločnosť pravidelne komunikovať s organizáciou, aby jej poskytovala aktuálne informácie o jej pokroku a akýchkoľvek problémoch, ktoré môžu nastať. Na uľahčenie tejto komunikácie by sa mal použiť plán komunikácie, ktorý bol vytvorený vo fáze vývoja plánu testovania.

Výstupy fázy

- Súbor podrobných informácií o výsledkoch testovania vrátane relevantných dôkazov o prítomnosti zistených zraniteľností.

4.1.7 Príprava záverečnej správy

Cieľ fázy

Táto kapitola načrtáva požiadavky na podávanie správ pre penetračné testovanie vrátane formátu správy, typov zistení, ktoré sa majú zahrnúť a informácií, ktoré majú byť do správy zahrnuté.

Popis fázy

Po dokončení testovacej fázy penetračný tester zostaví správu, ktorá dokumentuje zistené zraniteľnosti, použité techniky exploitovania a akékoľvek odporúčania na nápravu alebo ďalšie vylepšenia zabezpečenia. Správa sa zvyčajne predkladá klientovi alebo organizácii, ktorá si objednala služby penetračného testovania.

Kľúčovými komponentami typickej správy o penetračnom testovaní sú:

- Zhrnutie (pre manažment) - stručné zhrnutie procesu penetračného testovania, kľúčové zistenia a odporúčania. Táto časť je navrhnutá tak, aby poskytla prehľad obsahu správy vedúcim pracovníkom alebo zainteresovaným stranám, ktoré nemusia mať technické znalosti.
- Rozsah a metodika - opis metodiky testovania vrátane rozsahu testovania, použitých nástrojov a techník a akýchkoľvek obmedzení alebo predpokladov prijatých počas testovania.

- Posúdenie zraniteľnosti - komplexný zoznam všetkých zraniteľností objavených počas testovacej fázy, vrátane ich závažnosti, potenciálneho dopadu a pravdepodobnosti zneužitia.
- Výsledky exploitovania - podrobný popis techník exploitovania použitých počas testovania vrátane toho, ako bola každá zraniteľnosť zneužitá a úroveň získaného prístupu.
- Odporúčania - odporúčané nápravné opatrenia vrátane technických a procesných odporúčaní na zmiernenie zistených slabých miest.
- Záver - súhrn kľúčových zistení a odporúčaní vrátane všetkých nevyriešených problémov, ktoré si vyžadujú ďalšie skúmanie alebo nápravu.

Správa o penetračnom testovaní by mala byť jasná a stručná a mala by poskytovať dostatok podrobností, aby mohla organizácia podniknúť kroky na nápravu zistených zraniteľností. Mala by byť napísaná v jazyku, ktorý je prístupný technickým aj netechnickým zainteresovaným stranám. Správa je dôležitým výstupom, ktorý môže pomôcť organizáciám zlepšiť ich stav zabezpečenia a znížiť riziko úspešného kybernetického útoku.
Vzhľadom na charakter informácií v záverečnej správe z penetračného testu, by tento dokument mal byť klasifikovaný ako prísne chránený.

Výstupy fázy

- Záverečná správa s podrobnosťami o výsledkoch testovania vrátane zistených zraniteľností, rizík a odporúčaní na nápravu.

4.1.8 Kontrola výsledkov a prípadný re-test

Cieľ fázy

Táto kapitola sa zaoberá preskúmaním a overením záverečnej správy z penetračného testovania, potvrdením plánu nápravy a rozhodnutím o prípadnom re-teste .

Popis fázy

Po doručení správy je dôležité, aby organizácia na základe zistení prijala vhodné opatrenia. Nasledujúca kapitola načrtáva niektoré kľúčové kroky, ktoré by mala organizácia podniknúť, aby zo správy vyťažila maximum a rozhodla sa, či je potrebné opätovné testovanie.

Kontrola správy

Prvým krokom je dôkladné preskúmanie správy o penetračnom teste, aby boli pochopené zraniteľné miesta a riziká identifikované počas testovania. Správa by mala obsahovať podrobný popis testovacej metodiky, testovaných systémov a aplikácií a výsledky testovania vrátane všetkých zistených slabín a ich závažnosti.
Tiež je potrebné vykonať niekoľko kontrol:

- Kontrola úplnosti a presnosti - overenie, či boli testované všetky systémy a aplikácie a či sú v správe zahrnuté všetky zraniteľnosti identifikované počas testovania.
- Kontrola zistení– overiť, že zistenia sú založené na platných testovacích metodológiách a presne odrážajú závažnosť a potenciálny vplyv zistených zraniteľností.
- Kontrola odporúčaní – overiť, že poskytnuté odporúčania sú primerané a účinné pri riešení zistených slabých miest.

Prioritizácia zistení
Organizácia by mala prioritizovať zistenia na základe ich závažnosti a potenciálneho vplyvu na jej aktivity. Dá sa to dosiahnuť priradením skóre alebo úrovne rizika každému nálezu, pričom sa zohľadní pravdepodobnosť zneužitia zraniteľnosti a potenciálne dôsledky úspešného útoku.

Vypracovanie plánu nápravy
Na základe zistení zoradených podľa priorít by mala organizácia vypracovať plán nápravy na riešenie slabých miest a zmiernenie súvisiacich rizík. Plán by mal obsahovať konkrétne opatrenia, ktoré sa majú vykonať, harmonogramy dokončenia a zodpovedné strany. Je dôležité, aby sa do prípravy plánu zapojili kľúčové zainteresované strany.

Rozhodnutie pre opakovaný test (re-test)
Po vypracovaní a realizovaní plánu nápravy by sa mala organizácia rozhodnúť, či je potrebné opätovné testovanie. Zvyčajne sa odporúča opätovné otestovanie, aby sa potvrdilo, že slabé miesta boli úspešne odstránené, a aby sa zabezpečilo, že počas procesu nápravy neboli zavedené žiadne nové zraniteľnosti.

Rozhodnutie o opätovnom testovaní by malo brať do úvahy faktory, ako je závažnosť zraniteľností, zložitosť testovaných systémov a potenciálny vplyv úspešného útoku. Ak sa opätovné testovanie považuje za potrebné, organizácia by mala spolupracovať s externou spoločnosťou na plánovaní a vykonaní testovania.

Výstupy fázy

- Overenie slabých miest a rizík uvedených v správe.
- Vypracovanie a realizovanie plánu nápravy.
- Rozhodnutie o opätovnom testovaní

4.2 Zodpovednosti

Táto kapitola obsahuje súpis súvisiacich rol a ich zodpovednosti v súlade s definovanými činnosťami súvisiacimi s penetračným testovaním. Taktiež sú definované požiadavky na odbornosť, vzdelanie a skúsenosti penetračných testerov.

4.2.1 Zodpovednosti organizácie a dodávateľa služieb

Zodpovednosti organizácie:

- Sponzor projektu - schváli penetračné testovanie, poskytnite zdroje a urobí rozhodnutia súvisiace s testovaním.
- Manažér projektu - Spravuje projekt a zabezpečí, aby sa testovanie vykonávalo podľa rozsahu, požiadaviek a časovej osi.
- Právny tím - Skontroluje a schvaľuje zmluvy a dohody s dodávateľom služieb.
- Prevádzkový tím IT - Poskytne technickú podporu a zabezpečí, aby testovanie nenarušilo prevádzku organizácie.

Zodpovednosti dodávateľa služieb:

- Projektový manažér - riadi testovanie a zabezpečí, aby sa vykonávalo v súlade s rozsahom, požiadavkami a časovým plánom.

- Penetrační testeri - vykonajú testovanie podľa dohodnutej metodológie a identifikujú zraniteľné miesta a vektory útokov.
- Tím technickej podpory - poskytnite technickú podporu počas testovania a rieši technické problémy, ktoré môžu nastať.
- Reportovací tím – vypracuje správu z penetračného testovania na základe zistení z testovania.

4.2.2 Požiadavky na odbornosť, vzdelanie a skúsenosti penetračných testerov

Kľúčové zručnosti
Požadované zručnosti by mali byť vhodnou podmnožinou nasledovného zoznamu, reflektujúcou zameranie konkrétneho testera.
Penetračný tester by mal vedieť:

- Vyvíjať kódy, skripty a programy
- Vykonávať sociálne inžinierstvo
- Identifikovať a využívať zraniteľné miesta
- Vykonávať etický hacking
- Myslieť kreatívne
- Identifikovať a riešiť problémy súvisiace s kybernetickou bezpečnosťou
- Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám
- Efektívne využívať nástroje na penetračné testovanie
- Vykonávať technickú analýzu a podávanie správ
- Rozanalyzovať systémy s cieľom identifikácie slabých stránok a neúčinných kontrol
- Analyzovať zdrojové kódy a posúdiť ich bezpečnosť

Kľúčové znalosti
Požadované znalosti by mali byť vhodnou podmnožinou nasledovného zoznamu, reflektujúcou zameranie konkrétneho testera.
Penetračný tester by mal ovládať:

- Postupy kybernetického útoku
- Zariadenia informačných technológií (IT) a prevádzkových technológií (OT).
- Útočné a obranné bezpečnostné postupy
- Bezpečnosť operačných systémov
- Bezpečnosť počítačových sietí
- Postupy penetračného testovania
- Štandardy, metodológie a rámce penetračného testovania
- Nástroje na penetračné testovanie
- Počítačové programovanie
- Zraniteľnosti počítačových systémov
- Odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti
- Vlastniť certifikácie súvisiace s kybernetickou bezpečnosťou

5 Príklady nástrojov používaných pri penetračných testoch

Penetračné testovanie je zložitý proces, ktorý si vyžaduje použitie rôznych nástrojov a techník na identifikáciu a využitie zraniteľností v rámci systému alebo siete. Existuje mnoho rôznych typov penetračného testovania vrátane penetračného testovania siete, penetračného testovania webových aplikácií a penetračného testovania bezdrôtových sietí, pričom každý z nich vyžaduje špecifické nástroje a prístupy.

Výber nástrojov použitých na konkrétny penetračný test závisí od rôznych faktorov, ako je typ testovaného systému alebo aplikácie, metodika testovania a odbornosť testera. Niektoré populárne nástroje používané na penetračné testovanie zahŕňajú Metasploit, Nmap, Burp Suite, Wireshark a Aircrack-ng.

Je dôležité zvoliť vhodné nástroje pre konkrétny test, aby sa zabezpečili presné výsledky a efektívne identifikovali zraniteľné miesta. Použitie nesprávnych nástrojov môže viesť k nepresným alebo neúplným výsledkom, čo môže viesť k tomu, že kritické zraniteľnosti nebudú odhalené.

Celkovo je výber správnych nástrojov pre penetračný test rozhodujúci pre úspech testovacieho procesu a testeri musia starostlivo vyhodnotiť dostupné možnosti, aby vybrali tie najlepšie nástroje pre konkrétny vykonávaný test.

V nasledujúcej tabuľke sú uvedené príklady nástrojov pre rôzne typy penetračných testov:

Nástroj	Oblasť	Použitie
Nmap	Univerzálny	Nástroj na prieskum siete a bezpečnostný audit, ktorý možno použiť na skenovanie a mapovanie sietí, identifikáciu systémov a služieb a vykonávanie hodnotení zraniteľnosti.
Metasploit	Univerzálny	Nástroj na vývoj, testovanie a spúšťanie exploitov. Zahŕňa komplexnú zbierku exploitov a užitočných payloadov, ako aj výkonný skriptovací nástroj na automatizáciu rôznych úloh a vytváranie vlastných exploitov.
Wireshark	Univerzálny	Nástroj na analýzu sieťových protokolov, ktorý možno použiť na zachytávanie a kontrolu sieťovej prevádzky, identifikáciu a odstraňovanie problémov so sieťou a na vykonávanie hodnotení bezpečnosti.
Aircrack-ng	Bezdrôtový	Sada nástrojov na auditovanie bezpečnosti bezdrôtovej siete, ktoré možno použiť na zachytenie a analýzu prevádzky bezdrôtovej siete, vykonávanie útokov a hodnotenie bezpečnosti bezdrôtových sietí.
John the Ripper	Univerzálny	Nástroj na prelomenie hesiel, ktorý možno použiť na vykonávanie slovníkových útokov a útokov hrubou silou.
sqlmap	Infraštruktúra	Automatizovaný nástroj na SQL injekciu, ktorý možno použiť na objavovanie a využívanie zraniteľností SQL injekcie vo webových aplikáciách.
Nessus	Infraštruktúra, Sieť	Nástroj na skenovanie zraniteľností, ktorý možno použiť na vykonanie komplexných bezpečnostných testov, identifikáciu zraniteľností a stanovenie priorít pri odstraňovaní zistení.
Burp Suite	Webové aplikácie	Nástroj na testovanie bezpečnosti webových aplikácií, ktorý možno použiť na vykonávanie rôznych úloh, ako je skenovanie zraniteľností, skenovanie webových aplikácií a manuálne testovanie.
OWASP ZAP	Webové aplikácie	Nástroj na testovanie bezpečnosti webových aplikácií, ktorý možno použiť na vykonávanie rôznych úloh, ako je skenovanie zraniteľností, skenovanie webových aplikácií a manuálne testovanie.
Hashcat	Univerzálny	Nástroj na prelomenie hesiel, ktorý možno použiť na vykonávanie slovníkových útokov a útokov hrubou silou.

6 Kontrolný zoznam pre jednotlivé fázy penetračného testovania

Nasledujúca tabuľka uvádza prehľad výstupov pre jednotlivé fázy, pre jednoduchšiu kontrolu progresu počas penetračného testovania:

Fáza	Výstupy fázy
Definícia rozsahu a cieľov	• Popis rozsahu testovania. • Popis cieľov penetračného testovania.
Identifikácia požiadaviek	• Dokument popisujúci požiadavky a pravidlá zákazky
Výber externej spoločnosti	• Zoznam potenciálnych externých dodávateľov a ich kvalifikácie. • Užší zoznam externých dodávateľov, ktorí spĺňajú požiadavky organizácie. • Žiadosť na predloženie ponuky (RFP) • Výber externého dodávateľa.
Zmluvné a technické zabezpečenie penetračného testovania	• Zmluva s externým dodávateľom • Dohoda o mlčanlivosti (NDA) • Autorizačný list • Technické špecifikácie a požiadavky potrebné na vykonávanie penetračných testov.
Príprava plánu testov a komunikácie	• Plán testovania • Komunikačný plán
Testovanie	• Súbor podrobných informácií o výsledkoch testovania vrátane relevantných dôkazov o prítomnosti zistených zraniteľností
Príprava záverečnej správy	• Záverečná správa s podrobnosťami o výsledkoch testovania vrátane zistených zraniteľností, rizík a odporúčaní na nápravu.
Kontrola výsledkov a prípadný re-test	• Overenie slabých miest a rizík uvedených v správe. • Vypracovanie a realizovanie plánu nápravy. • Rozhodnutie o opätovnom testovaní

7 Prílohy

Prílohy obsahujú ukážky uvedených dokumentov.

7.1 Príloha 1 - Príklad správy

7.2 Príloha 2– Príklad autorizačného listu

7.3 Príloha 3 – Príklad dohody o mlčanlivosti (NDA)