pragodata

SLUŽBY PENETRAČNÍHO TESTOVÁNÍ

NÚKIB definuje Penetrační testování a testování zranitelností jako jednu z povinností vyplývajících z vyhlášky **č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.**

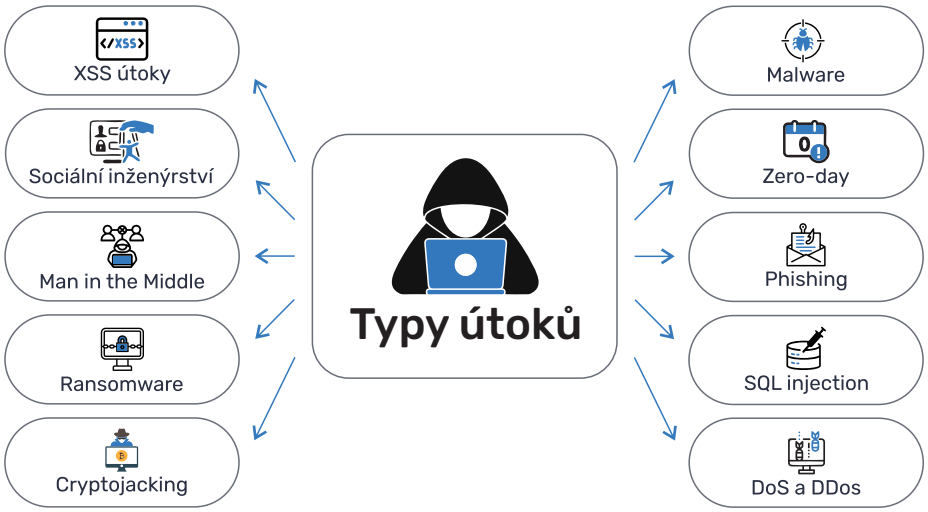
NABÍDKA TESTŮ

EXTERNÍ PENETRAČNÍ TESTY:

- **Testy webových aplikací**
- **Testy mobilních aplikací**
- **Information gathering** *(OSINT)*
- **Testy perimetru** *(firewall, DMZ, DNS, ...)*
- **Testy e-mail systému** *(DMARC, ...)*
- **Phishingové testy** *(spear phishing)*

INTERNÍ PENETRAČNÍ TESTY:

- **Testy infrastruktury** *(VLANy, WiFi, virtualizace, ...)*
- **Testy stanic a Active Directory** *(konfigurace, hesla, ransomware, ...)*
- **Testy a audity serverů** *(Linux a Microsoft)*
- **Testy a audity e-mail serverů** *(cloud, lokální, sandboxing, ...)*



TYPY TESTŮ

Black-box testy

Black-box testy simulují vnější přístup útočníka, který zná jenom obecné informace, ale nikoliv vnitřní strukturu aplikace, serveru nebo sítě. Samotná funkcionalita systému je pro testera černou skříňkou (angl. black-box).

White-box testy

V porovnání s předchozím typem testů (black-box) jsou pro tyto testy typické vstupní znalosti. Takový druh testů vyžaduje dokumentaci o testovaných aplikacích, serverech nebo sítích.

Grey-box testy

Jedná se o kombinaci výše již zmíněných testů. Testerovi je poskytnuta jen částečná znalost testovaného systému a následně postupuje jako při black-box testování.

pragodata

DOPORUČENÉ POSTUPY PO TESTOVÁNÍ

- Na základě vyhodnocení výsledků penetračního testování, by mělo dojít k **bezodkladnému odstranění nalezených nedostatků**.
- Po prvním penetračním testování je zpravidla odhaleno velké množství **reálně zneužitelných zranitelností** zabezpečení. V případě, že dojde k důslednému odstranění zjištěných nedostatků, každé další penetrační testování by mělo odhalit menší množství reálně zneužitelných zranitelností, o to větší je však efekt na praktické zabezpečení celého systému.
- Pokud nebude organizace **adekvátně reagovat** na vyšledky penetračního testování, resp. nebude realizovat odstranění zjištěných nedostatků, pak samotné provedení penetračního testování nebude mít žádnou přidanou hodnotu pro správce systému.

VYHODNOCENÍ ZRANITELNOSTI DLE STUPNĚ ZÁVAŽNOSTI

KRITICKÉ	VYSOKÉ	STŘEDNÍ	NÍZKÉ
Odhalené zranitelnosti je možné okamžitě využít na kompletní kompromitování systému.	Odhalené zranitelnosti, které v kombinaci s jinými zranitelnostmi nebo postupy („sociální inženýring"), představují vysoké riziko.	Musí být splněné speciální podmínky pro zneužití uvedených zranitelností nebo jejich případné zneužití má omezený dopad.	Drobné bezpečnostní problémy.

VÝSTUPY Z PENETRAČNÍCH TESTŮ

- Výstupem Penetračních testů je **závěrečná zpráva** - dokument popisující stav daných oblastí IS z pohledu bezpečnosti s návrhem doporučení. Výsledná zpráva obsahuje pro každou testovanou IP adresu/server datum a čas testování, odhalenou verzi OS a seznam zranitelností s různým **stupněm závažnosti**.

- Zpráva dále obsahuje manažerské shrnutí a výsledky testů pro jednotlivé aplikace, služby či systémy. Výsledky obsahují seznam odhalených **zranitelností** seřazených podle stupně závažnosti – od kritických zranitelností, přes zranitelnosti s vysokým, středním a nízkým stupněm závažnosti. Ke každé odhalené zranitelnosti je uveden **detailní popis**, **stupeň závažnosti** a **doporučení** jak uvedenou zranitelnost opravit.

- Dodavatel v maximální míře zabezpečí, aby testování bylo **nedestruktivní** a **nezpůsobilo pády systémů, úpravu nebo smazání dat**. Toto neplatí v případě modifikace dat, například logů, které jsou způsobené normálním použitím systému (například nárůst přístupových logů).

- Postup testování vychází z metodik **OSSTMM, OWASP, PTES, NIST 800-115** a doporučení **NÚKIB**.

SOUČINNOST ZÁKAZNÍKA

Pro úspěšnou realizaci v daných termínech a řádné zajištění podpůrných služeb je nezbytné poskytnutí součinnosti ze strany zákazníka a to především:

- Specifikovat **aplikace a příslušné servery** pro účely testování (IP adresy, názvy serverů).
- Specifikovat a poskytnout vhodný **časový rámec** pro testy.
- Definovat **IP adresy** zařízení, které mají specifické požadavky na realizaci testů (doba realizace, případně další omezení).
- Vytvořit **vhodné virtuální prostředí** v interní síti zákazníka, ze kterého budou spouštěny automatizované nástroje pro testování.
- Naplňovat **obecné zásady** řízení projektu a vytvářet předpoklady pro plnění závazků vyplývajících z realizovaných dohod tak, aby nedocházelo k prodlení s plněním jednotlivých termínů pro poskytnutí plnění.
- V průběhu jednotlivých činností budou po předchozí dohodě k dispozici zainteresovaní **zástupci zákazníka**, tj. poskytnout kontaktní informace (mobily a e-maily na administrátory zákazníka).
- Zajistit **podporu managementu** zákazníka pro celou dobu projektu.
- Zajistit poskytování **úplných, pravdivých a včasných informací**, které jsou nebo by mohly být potřebné k řádnému plnění závazků dodavatele.
- Zajistit **poskytnutí veškerých informací**, podkladů, interních dokumentů, zákonných norem, předpisů, směrnic, pokynů a metodických předpisů souvisejících nebo ovlivňujících problematiku řízení provozu IT a bezpečnosti. Předání těchto materiálů zajistí Oprávněná osoba zákazníka, a to nejpozději do 2 dnů od podpisu Smlouvy / Objednávky nebo do 2 dnů od oficiální žádosti SONPO.
- Účastnit se **naplánovaných jednání**, telekonferencí a řešit řádně a včas přidělené úkoly.