Autonomní Penetrační Testy

Profesionální penetrační test představuje pro firmy významnou hodnotu,protože identifikuje možné vektory útoku a přináší důkaz o jejich zneužitelnosti. Může stejně tak i potvrdit, že obranné mechanismy jsou implementovány efektivně, a zaměřit se na nápravu nejkritičtějších slabin organizace.

Existují dva základní typy penetračních testů: externí penetrační testy, které mají zajistit silný perimetr, a interní penetrační testy, které mají odhalit slabá místa, jež by mohl využít útočník, který se již dostal do sítě.

Ověřujte své zabezpečení průběžně

Jste si jisti, že jste dostatečně zabezpečení? Nečekejte, až dojde k narušení, abyste to zjistili. Průběžně testujte své zabezpečení, abyste zajistili, že žádná zneužitelná zranitelnost, chybná konfigurace nebo získané heslo vás nevystaví riziku. Externí pentesty prověřují vaše veřejně dostupná aktiva s cílem zjistit, jakým způsobem může být protivník schopen identifikovat a zneužít slabá místa pro vstup do vaší sítě.

Externí penetrační testy identifikují vektory útoku, které zahrnují:

- **Otevřené porty a chybné konfigurace, které umožňují útočníkovi proniknout do sítě.**
- **Neopravené zranitelnosti, které lze zneužít k přístupům neautentizovaných uživatelů.**
- **Shadow IT projekty, které rozšiřují možnosti k útoku.**

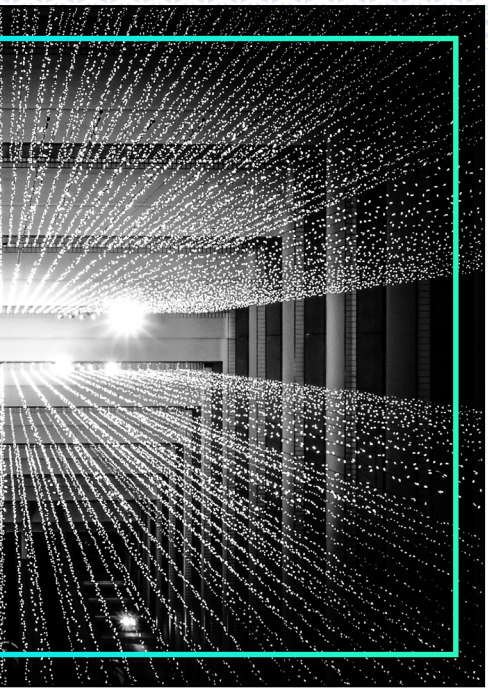
Předpokládejte průlom abyste omezili škody

V dnešním době neustálých phishingových útoků, dostupnosti ukradených přihlašovacích údajů a špatně zabezpečených systémů musíte předpokládat, že k počátečnímu narušení již došlo a útočníci již mají přístup do vašich interních systémů.

Interní penetrační test začíná předpokladem, že útočník má přístup do vaší sítě, kde se nachází vaše citlivá data. Kromě vektorů útoku, které jsou stejné jako u externích testů, interní penetrační testy určují, čeho může záškodník z tohoto výchozího bodu dosáhnout:

- **Jak mohou získat přístup k dalším heslům a oprávněním?**
- **Jaké slabiny a zranitelnosti mohou využít k dalšímu pohybu?**
- **K jakým citlivým datům se dostanou?**
- **Které konkrétní problémy je třeba odstranit - a jak - aby se zabránilo útoku?**

NZ není skener zranitelností



Skenery zranitelností prohledávají perimetr a interní systémy a hledají nezáplatované aplikace. Spouští pravidla pro vyhledávání známých zranitelností, které jsou v seznamu CVE (Common Vulnerabilities and Exposures) organizace NIST. Výsledkem je většinou zpráva s mnoha nálezy s nízkou prioritou. Ty dokáží zaměstnat týmy řešením nezneužitelných problémů místo toho, aby se zaměřily na nejkritičtější zranitelnosti.

Je také důležité vědět, že skenery zranitelností neidentifikují nesprávně záplatované systémy a nedokáží identifikovat útočné cesty, při kterých útočník může řetězit a kombinovat několik zranitelností za sebou.

Vulnerable ≠ Exploitable

Oproti tomu NodeZero identifikuje slabá místa ve vašich externích, lokálních a cloudových systémech i u vašich uživatelů, a to i v případě, že skenery zranitelností a systémy správy záplat ukazují, že aktualizace zabezpečení proběhly úspěšně. Poskytuje detailní popis útoku krok za krokem a také důkaz každého úspěšného zneužití. Tak pochopíte, jak může útočník zaútočit a dozvíte se jaká učinit opatření, abyste těmto útokům předešli. NodeZero vám umožní prioritizovat tak, abyste přednostně věnovali čas kritickým problémům a upozadili zranitelnosti, které nejsou zneužitelné.

NodeZero

Zabezpečení prověřujte průběžně. NodeZero řeší problém nákladného a manuálního penetračního testování tím, že tento proces automatizuje.

NodeZero je autonomní pentester - "samoobslužné" řešení, které lze bezpečně provozovat v produkci a které nevyžaduje přípravné zásahy či hesla. Posuzuje systémy stejně jako manuální pentester, ale rychleji, úplněji a s použitelnějšími výsledky.

~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

HORIZON3.ai
~~TRUST BUT~~ VERIFY

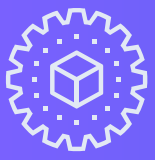
Co je Autonomní Penetrační Testování?

NodeZero se od ostatních nástrojů liší tím, že kombinuje nižší náklady a vysokou frekvenci testování s odbornými znalostmi, důkladností a přesností manuálních testů prováděných vysoce kvalifikovanými bezpečnostními odborníky. Výsledkem je možnost provádět nepřetržitá "purple teaming" cvičení s nízkými ročními náklady. Penetrační testy se vyvinuly od manuálních přes crowdsourcované, automatizované, až k **autonomním.**

Manuální pentest vyžaduje odborníka se specializovanými, mnohdy komerčními nástroji pro průzkum aplikace nebo systému a identifikaci slabých míst. Efektivita a náklady tohoto testu závisí na čase a dovednostech pentestera, což vede mnoho společností k tomu, že poskytnou testerovi základní přístupy.
Výsledky jsou čistší než u automatizovaného pentestu, ale výsledný report bývá příliš stručný. Vysoké náklady na manuální pentesty brání společnostem v jejich častém používání, například po každém patchování systému, aby se ujistily, že bylo vše provedeno správně.

Automatický pentest je jednoduchý přístup na principu "point and click" využívající komerční nástroje pro dynamickou analýzu.
Nástroj dostane URL nebo IP adresu, aplikaci prohledá a odhalí místa, kam je možné zadat uživatelské vstupy. Nástroj následně zkouší různé typy vstupů, aby nalezl možné zranitelnosti. Zkušený útočník dokáže nálezy následně zneužít případně zahltit aplikaci DoS útokem. Tyto testy typicky trvají den či dva a vytváří velké množství šumu, který je třeba dále analyzovat, aby bezpečnostní tým kvalifikovaně rozhodl, jestli je třeba nálezy dále řešit.

Crowdsourced pentest zahrnuje manuální pentesty, ale spoléhá na síť nezávislých bezpečnostních výzkumníků, kteří jsou placeni za nalezené zranitelnosti (plus poplatek provozovateli platformy). Crowdsourced pentesty mají výhodu v otevřenosti - teoreticky lidé mohou hledat zranitelnosti mnoho dnů a měsíců. Tento přístup může být drahý, pokud je nalezeno velké množství zranitelností bez důkazu možného zneužití. Vývojové týmy tak opět mohou trávit čas na nekritických nálezech. Těmto programům se také říká Bug Bounty programy.



Autonomní pentest kombinuje výhody automatického pentestu (častější testování, nižší náklady, a nulové požadavky na interní bezpečnostní expertizu) s výhodami manuálního pentestu (rozsáhlejší pokrytí aplikace a prokázání zneužitelnosti). Autonomní pentest nevyžaduje ke spuštění přihlašovací údaje. Dokáže řetězit zranitelnosti jako zkušený útočník a vygenerovat strom úspěšného útoku k identifikaci hlavní příčiny. Tato srozumitelná dokumentace umožňuje uživateli přesně pochopit, co je třeba změnit, aby byl systém správně chráněn.

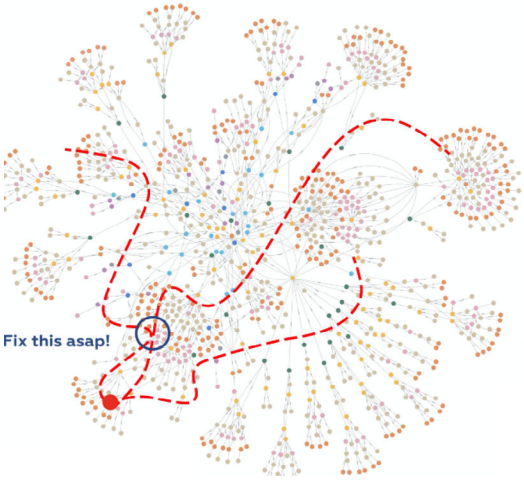
HORIZON3.ai
~~TRUST~~ BUT VERIFY

Jak NodeZero funguje?

Průzkum
Každý úspěšný útok vyžaduje dobré informace o cíli. NodeZero začíná s neautentizovaným přístupem do systému, pak vytvoří Knowledge Graph, identifikuje všechny hostitele, chybné konfigurace, otevřené porty a hledá přístupové údaje.

Maneuver Loop
NodeZero využívá k provedení útoku přes 100 nástrojů ke sběru hesel, zneužití zranitelností, zneužití výchozího nebo chybného nastavení.

Ověřené cesty útoku
Pro zjednodušení prioritizace oprav jsou výsledky prezentovány jako důkazy s grafickým a textovým vysvětlením každého kroku úspěšného útoku. Toto zahrnuje popis použité taktiky, jaké zranitelnosti byly nalezeny a zneužity, jak se podařilo získat přihlašovací údaje a cesty k získání práv a přístupu do systému.



Dopad
NodeZero informuje o všech datech na fyzických a virtuálních prostředích, ke kterým se bylo možné dostat s právy čtení/zápisu, včetně sdílení SMB a NFS, FTP, cloudových úložišť, serverů vCenter a databází.

Kontextový Skóring
NodeZero vyhodnocuje a prioritizuje slabiny na základě jejich možné role v útoku, nikoli dle CVSS skóre.

Uživatel díky tomu rychle identifikuje slabiny, které představují momentálně nejvyšší hrozbu a musí být řešeny okamžitě a ty, které lze bezpečně odložit na později.

Srozumitelné pokyny k nápravě
NodeZero poskytuje přesné pokyny k odstranění nalezených zranitelností. Pro vaše týmy je pak jejich realizace snadná a nevyžaduje podrobnější studium či expertizu.

Test místo slibů!

NodeZero je Autonomní Penetrační Testovací nástroj, který pomáhá společnostem najít a ošetřit možné cesty útoku dříve, než je zneužije útočník.
Je bezpečný v produkčním prostředí a nevyžaduje žádné agenty nebo přístupy na cílová zařízení.

Kontaktujte nás pro ukázku ve Vaší síti.
https://www.sec4good.cz

© 2023 Sec4good @sec4good info@sec4good.cz www.sec4good.cz